STATE OF CALIFORNIA
STANDARD AGREEMENT
STD 213_DHCS (Rev. 06/16)

REGISTRATION NUMBER	AGREEMENT NUMBER
	17-94146

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

STATE AGENCY'S NAME (Also known as DHCS, CDHS, DHS or the State)
Department of Health Care Services

CONTRACTOR'S NAME (Also referred to as Contractor)
County of Nevada

2. The term of this Agreement is: July 1, 2017 through June 30, 2020

3. The maximum amount of this Agreement is: **$** 2,113,050
Two Million, One Hundred Thirteen Thousand, Fifty Dollars

4. The parties agree to comply with the terms and condition of the following exhibits, which are by this reference made a part of this Agreement.

Exhibit A – Scope of Work	2 pages
Exhibit A, Attachment I – Program Specifications	22 pages
Exhibit B – Budget Detail and Payment Provisions	13 pages
Exhibit B, Attachment I – Funding Amounts	1 page
Exhibit C * – General Terms and Conditions	GTC 04/2017
Exhibit D (F) – Special Terms and Conditions	26 pages
Exhibit E – Additional Provisions	3 pages
Exhibit F – Privacy and Information Security Provisions	28 pages
Exhibit F, Attachment I – Social Security Administration Agreement	101 pages

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CONTRACTOR'S NAME *(if other than an individual, state whether a corporation, partnership, etc.)*
County of Nevada

BY *(Authorized Signature)* ✍ | DATE SIGNED *(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING
Hank Weston, Chair. Board of Supervisors

ADDRESS
500 Crown Point Circle
Grass Valley, CA 95945

STATE OF CALIFORNIA

AGENCY NAME
Department of Health Care Services

BY *(Authorized Signature)* ✍ | DATE SIGNED *(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING
Don Rodriguez, Chief, Contract Management Unit

ADDRESS
1501 Capitol Avenue, Suite 71.2048, MS 1400, P.O. Box 997413,
Sacramento, CA 95899-7413

California Department of General Services Use Only

[X] Exempt per: DGS memo dated 07/10/96 and Welfare and Institutions Code 14087.4

Exhibit A
Scope of Work

1. Service Overview

Contractor agrees to provide to the California Department of Health Care Services (DHCS) the services described herein.

DHCS and the Contractor enter into this Contract by authority of Chapter 3 of Part 1, Division 10.5 of the Health and Safety Code (HSC) for the purpose of providing alcohol and other drug prevention, treatment and recovery support services. DHCS and the Contractor identified in the Standard Agreement are the only parties to this Contract. This Contract is not intended, nor shall it be construed, to confer rights on any third party.

DHCS and the Contractor enter into this Contract by authority of Title 45 of the Code of Federal Regulations Part 96 (45 CFR Part 96), Substance Abuse Prevention and Treatment Block Grants (SABG) for the purpose of planning, carrying out, and evaluating SABG authorized activities to prevent and treat substance abuse. SABG recipients must adhere to SAMHSA's National Outcome Measures (NOMs).

The objective is to prevent and treat substance abuse through utilization of Federal SABG funds pursuant to Section 1921 of Title XIX, Part B, Subpart II and III of the Public Health Service (PHS) Act, for services rendered by county operated or county contracted substance use disorder service providers.

2. Service Location

The services shall be performed at applicable facilities in the County of Nevada.

3. Service Hours

The services shall be provided during the working hours and days as defined by the Contractor.

4. Project Representatives

A. The project representatives during the term of this Agreement will be:

Department of Health Care Services	**County of Nevada**
Contract/Grant Manager: Robert Strom Telephone: (916) 327-2696 Fax: (916) 322-1176 Email: Robert.Strom@dhcs.ca.gov	Rebecca Slade, LMFT, Director of Behavioral Health Telephone: (530) 265-1437 Fax: 530-271-0257

Exhibit A
Scope of Work

B. Direct all inquiries to:

Department of Health Care Services	**County of Nevada**
Department of Health Care Services SUD PPFD - PSGMB Attention: Nancy Shinn Mail Station Code 2624 P.O. Box 997413 Sacramento, CA, 95899-7413 Telephone: (916) 322-9677 Fax: (916) 323-1176 Email: Nancy.Shinn@dhcs.ca.gov	Nevada Behavioral Health Care Services Attention: Rebecca Slade, LMFT, Director of Behavioral Health 500 Crown Point Circle Grass Valley, CA 95945 Telephone: (530) 265-1437 Fax: 530-271-0257

C. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement.

5. Americans with Disabilities Act

Contractor agrees to ensure that deliverables developed and produced, pursuant to this Agreement shall comply with the accessibility requirements of Section 508 of the Rehabilitation Act and the Americans with Disabilities Act of 1973 as amended (29 U.S.C. § 794 (d), and regulations implementing that act as set forth in Part 1194 of Title 36 of the Federal Code of Regulations. In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code section 11135 codifies section 508 of the Act requiring accessibility of electronic and information technology.

6. See Exhibit A, Attachment I, for a detailed description of the services to be performed.

Exhibit A, Attachment I
Program Specifications

Part I - Substance Use Disorder Prevention and Treatment Block Grant Services

Section 1 - Formation and Purpose

A. Authority

1. This Exhibit A, Attachment I, Part I of the Contract is entered into by and between the Department of Health Care Services (DHCS) and the Contractor, under the authority of Chapter 3 of Part 1, Division 10.5 of the Health and Safety Code (HSC), and with the approval of Contractor's County Board of Supervisors (or designee), for the purpose of providing alcohol and drug services, and shall be reimbursed pursuant to Exhibit A, Attachment I. DHCS and the Contractor identified in the Standard Agreement are the sole parties to this Contract. This Contract is not intended, nor shall it be construed, to confer rights on any third party.

B. Federal Award Subrecipient

1. The Substance Abuse Prevention and Treatment Block Grant (SABG) is a federal award within the meaning of Title 45, Code of Federal Regulations (CFR), Part 75. This Contract is a subaward of the federal award to DHCS.

2. Contractor is a subrecipient and subject to all applicable administrative requirements, cost principles, and audit requirements that govern federal monies associated with the SABG set forth in the Uniform Guidance 2 CFR Part 200, as codified by Health and Human Services (HHS) at 45 CFR Part 75.

3. As a subrecipient, the Contractor shall:

   a) Maintain effective internal control over the SABG funds.

   b) Comply with federal statutes, regulations, including 45 CFR Part 75, and terms and conditions of the SABG grant.

   c) Evaluate and monitor its activities and the activities of all subcontractors for compliance with applicable statutes, regulations, and terms and conditions of the subaward.

   d) Address any instances of noncompliance promptly, including noncompliance identified in audit findings.

4. The Contractor shall disclose, in writing to DHCS, any potential conflict of interest in accordance with Health and Human Services' (HHS) grant policy. (See, https://www.hhs.gov/sites/default/files/grants/grants/policies-regulations/hhsgps107.pdf).

5. The Contractor shall timely disclose, in writing to DHCS, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the grant. If the Contractor fails to make a required disclosure, DHCS may seek those remedies described in 45 CFR Section 75.371.

6. The Contractor shall have a single audit performed in accordance with the audit requirements set forth in 45 CFR Part 75, Subpart F.

Exhibit A, Attachment I
Program Specifications

C. Control Requirements

1. Performance under the terms of this Exhibit A, Attachment I, Part I, is subject to all applicable federal and state laws, regulations, and standards. In accepting DHCS drug and alcohol SABG allocation pursuant to HSC Sections 11814(a) and (b), Contractor shall: (i) establish, and shall require its subcontractors to establish, written policies and procedures consistent with the control requirements set forth below; (ii) monitor for compliance with the written procedures; and (iii) be accountable for audit exceptions taken by DHCS against the Contractor and its subcontractors for any failure to comply with these requirements:

   a) HSC, Division 10.5, Part 2 commencing with Section 11760.

   b) Title 9, California Code of Regulations (CCR) (herein referred to as Title 9), Division 4, commencing with Section 9000.

   c) Government Code, Title 2, Division 4, Part 2, Chapter 2, Article 1.7.

   d) Government Code, Article 7, Federally Mandated Audits of Block Grant Funds Allocated to Local Agencies, Chapter 1, Part 1, Division 2, Title 5, commencing at Section 53130.

   e) Title 42 United State Code (USC), Sections 300x-21 through 300x-31, 300x-34, 300x-53, 300x-57, and 330x-64 through 66.

   f) Title 2, CFR 200 -The Uniform Administration Requirements, Cost Principles and Audit Requirements for Federal Awards.

   g) Title 45, Code of Federal Regulations (CFR), Sections 96.30 through 96.33 and Sections 96.120 through 96.137.

   h) Title 42, CFR, Sections 8.1 through 8.6.

   i) Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2, Subparts A – E).

   j) Title 21, CFR, Sections 1301.01 through 1301.93, Department of Justice, Controlled Substances.

   k) State Administrative Manual (SAM), Chapter 7200 (General Outline of Procedures).

   Contractor shall be familiar with the above laws, regulations, and guidelines and shall assure that its subcontractors are also familiar with such requirements.

2. The provisions of this Exhibit A, Attachment I, Part I, are not intended to abrogate any provisions of law or regulation, or any standards existing or enacted during the term of this Contract.

3. Contractor shall adhere to the applicable provisions of Title 45, CFR, Part 96, Subparts C and L, as applicable, in the expenditure of SABG funds. Document 1A, 45 CFR 96, Subparts C and L, is incorporated by reference.

4. Driving-Under-the-Influence Program Requirements (Documents 1C) contains additional requirements that shall be adhered to by the Contractor.

5. Contractor and all its subcontractors shall comply with the Minimum Quality Drug Treatment Standards for SABG for all Substance Use Disorder (SUD) treatment programs either partially or fully funded by SABG. The Minimum Quality Drug Treatment Standards for SABG are attached to this Contract as Document 2F(b), incorporated by reference. The incorporation of any new Minimum Quality Drug Treatment Standards into this Contract shall not require a formal amendment.

Section 2 – General Provisions

A. Restrictions on Salaries

Contractor agrees that no part of any federal funds provided under this Contract shall be used by the Contractor or its subcontractors to pay the salary and wages of an individual at a rate in excess of Level I of the Executive Schedule. Salary and wages schedules may be found at https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/17Tables/exec/html/EX.aspx. SABG funds used to pay a salary in excess of the rate of basic pay for Level I of the Executive Schedule shall be subject to disallowance. The amount disallowed shall be determined by subtracting the individual's actual salary from the Level I rate of basic pay and multiplying the result by the percentage of the individual's salary that was paid with SABG funds (Reference: Terms and Conditions of the SABG award).

B. Primary Prevention

1. The SABG regulation defines "Primary Prevention Programs" as those programs "directed at individuals who have not been determined to require treatment for substance abuse" (45 CFR 96.121), and "a comprehensive prevention program which includes a broad array of prevention strategies directed at individuals not identified to be in need of better treatment" (45 CFR 96.125). Primary prevention includes strategies, programs and initiatives which reduce both direct and indirect adverse personal, social, health, and economic consequences resulting from problematic Alcohol and Other Drug (AOD) availability, manufacture, distribution, promotion, sales, and use. The desired result of primary prevention is to promote safe and healthy behaviors and environments for individuals, families and communities. The Contractor shall expend not less than its allocated amount of the SABG Primary Prevention Set-Aside funds on primary prevention as described in the SABG requirements (45 CFR 96.124).

2. Contractor is required to have a current and DHCS approved County Strategic Prevention Plan (SPP). The SPP must demonstrate that the County utilized the Substance Abuse and Mental Health Services Administration's Strategic Prevention Framework (SPF) in developing the plan as described at http://www.samhsa.gov/capt/applying-strategic-prevention-framework. DHCS will only approve SPP's that demonstrate that the Contractor utilized the SPF. Contractor shall:

   a) Follow DHCS guidelines provided in the SPP Guide (Document 1N, incorporated by reference) and the Strategic Prevention Plan Workbook for Counties Utilizing the Strategic Prevention Framework (Document 1O, incorporated by reference).

b) Prepare a new SPP by October 1 of the year prior to the expiration date of the current SPP.

c) Submit a timeline, no later than October 1 of the year prior to the expiration date of the current SPP, for approval to DHCS that includes proposed dates for submitting each section of the SPP (outlined in the SPP Guide and the SPP Workbook).

d) Submit drafts of each SPP section to DHCS for review and approval according to the approved timeline.

e) Submit a completed draft of the SPP to DHCS no later than May 31st that includes the previously approved sections for final review and approval.

f) Provide an electronic copy of the final SPP to DHCS within 10 business days of approval and input planning data from the approved SPP into the prevention data collection service as requested.

3. Contractor shall submit a Prevention Mid-Year Budget to DHCS by January 31 of each fiscal year. The budget shall forecast how the SABG Primary Prevention Set-Aside funds will be expended for the fiscal year.

C. Friday Night Live

Contractors and subcontractors receiving SABG Friday Night Live (FNL) funding must:

1. Engage in programming that meets the FNL Youth Development Standards of Practice, Operating Principles and Core Components outlined at http://fridaynightlive.org/about-us/cfnlp-overview/.

2. Use the prevention data collection and reporting service for all FNL reporting including profiles and chapter activity.

3. Follow the FNL Data Entry Instructions for the prevention data collection and reporting service as provided by DHCS.

4. Meet the Member in Good Standing (MIGS) requirements, as determined by DHCS in conjunction with the California Friday Night Live Collaborative and the California Friday Night Live Partnership. Contractors that do not meet the MIGS requirements shall obtain technical assistance and training services from the California Friday Night Live Partnership and develop a technical assistance plan detailing how the Contractor intends to ensure satisfaction of the MIGS requirements for the next review.

D. Perinatal Services Network Guidelines

Contractor shall comply with the perinatal program requirements as outlined in the Perinatal Services Network Guidelines. The Perinatal Services Network Guidelines 2016-17 are attached to this Contract as Document 1G, incorporated by reference. The Contractor shall comply with the current version of these guidelines until new Perinatal Services Network Guidelines are established and adopted. The incorporation of any new Perinatal Services Network Guidelines into this Contract shall not require a formal amendment. Contractor receiving SABG funds must adhere to the Perinatal Services Network Guidelines, regardless of

whether the Contractor exchanges perinatal funds for additional discretionary funds.

E. Funds identified in this Contract shall be used exclusively for county alcohol and drug abuse services to the extent activities meet the requirements for receipt of federal block grant funds for prevention and treatment of substance abuse described in subchapter XVII of Chapter 6A of Title 42, the USC.

F. Room and Board for Transitional Housing

Contractor may use SABG discretionary funds to cover the cost of room and board of residents living in temporary, drug and alcohol free, transitional housing if the resident is actively engaged in treatment for a medically necessary SUD provided to the resident off-site. Contractor shall develop guidelines for contracted housing providers and provide monitoring and oversight and fulfill all SABG reporting requirements. Contractors and subcontractors using SABG discretionary funds to cover the cost of room and board for transitional housing shall:

1. Facilitate the beneficiary's movement in recovery from a SUD to independent living and integration into post treatment return or re-entry into the community.

2. Require that all individuals in the transitional housing be engaged in SUD treatment, off-site, at all times during the individual's stay.

3. Ensure payment of room and board expenses for a residential stay be limited to short term (up to 24 months).

4. Ensure the transitional housing be secure, safe, and alcohol and drug free.

Section 3 - Performance Provisions

A. Monitoring

1. Contractor's performance under this Exhibit A, Attachment I, Part I, shall be monitored by DHCS during the term of this Contract. Monitoring criteria shall include, but not be limited to:

   a) Whether the quantity of work or services being performed conforms to Exhibit B.

   b) Whether the Contractor has established and is monitoring appropriate quality standards.

   c) Whether the Contractor is abiding by all the terms and requirements of this Contract.

   d) Whether the Contractor is abiding by the terms of the Perinatal Services Network Guidelines (Document 1G).

   e) Whether the Contractor conducted annual onsite monitoring reviews of services and subcontracted services for programmatic and fiscal requirements. Contractor shall submit copy of its monitoring and audit reports to DHCS within two weeks of issuance.

Reports should be sent by secure, encrypted e-mail to:

SUDCountyReports@dhcs.ca.gov or

Substance Use Disorder – Program, Policy, and Fiscal Division
Performance Management Branch
Department of Health Care Services
PO Box 997413, MS-2627
Sacramento, CA 95899-7413

2. Failure to comply with the above provisions shall constitute grounds for DHCS to suspend or recover payments, subject to the Contractor's right of appeal, or may result in termination of the Contract or both.

B. Performance Requirements

1. Contractor shall provide services based on funding set forth in Exhibit B, Attachment I and under the terms of this Contract.

2. Contractor shall provide services to all eligible persons in accordance with federal and state statutes and regulations. Contractor shall assure that in planning for the provision of services, the following barriers to services are considered and addressed:

   a) Lack of educational materials or other resources for the provision of services.

   b) Geographic isolation and transportation needs of persons seeking services or remoteness of services.

   c) Institutional, cultural, and/or ethnicity barriers.

   d) Language differences.

   e) Lack of service advocates.

   f) Failure to survey or otherwise identify the barriers to service accessibility.

   g) Needs of persons with a disability.

3. Contractor shall comply with any additional requirements of the documents that have been incorporated herein by reference, including, but not limited to, those on the "List of Exhibit A, Attachment I Documents incorporate by Reference for Fiscal Year 2017-18" which is attached to Exhibit A, Attachment I.

4. The funds described in Exhibit A, Attachment I shall be used exclusively for providing alcohol and/or drug program services.

5. DHCS shall issue a report to Contractor after conducting monitoring, utilization, or auditing reviews of the county or county subcontracted providers. When the DHCS report identifies non-compliant services or processes, it shall require a Corrective Action Plan (CAP). The Contractor in coordination with its subcontracted provider shall submit a CAP to DHCS

within the designated timeframe specified by DHCS. The CAP should be sent by secure, encrypted e-mail to: SUDCountyReports@dhcs.ca.gov or

Substance Use Disorder - Program, Policy, and Fiscal Division
Performance Management Branch
Department of Health Care Services
PO Box 997413, MS-2621
Sacramento, CA 95899-7413

6. The CAP shall include:

   a) A statement of the deficiency.

   b) A list of action steps to be taken to correct the deficiency.

   c) A date of completion for each deficiency corrected.

   d) Who will be responsible for correction and ongoing compliance.

7. DHCS will provide written approval of the CAP to the Contractor within 30 calendar days. If DHCS does not approve the CAP submitted by the Contractor, DHCS will provide guidance on the deficient areas and request an updated CAP from the Contractor with a new deadline for submission.

8. If the Contractor does not submit a CAP, or, does not implement the approved CAP provisions within the designated timeline, then DHCS may withhold funds until the Contractor is in compliance. DHCS shall inform the Contractor when funds will be withheld.

C. Sub-recipient Pre-Award Risk Assessment

Contractor shall comply with the sub-recipient pre-award risk assessment requirements contained in 2 CFR Part 200 Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards. Contractor, as the SABG first-tier sub-recipient, shall review the merit and risk associated with all potential grant second-tier sub-recipients (subcontractors) annually prior to making an award. Contractor shall perform and document annual sub-recipient pre-award risk assessments for each subcontractor and retain documentation for audit purposes.

Section 4 - Investigations and Confidentiality of Administrative Actions

A. Contractor shall execute the Confidentiality Agreement, attached as Document 5A. The Confidentiality Agreement permits DHCS to communicate with Contractor concerning subcontracted providers that are subject to administrative sanctions.

Exhibit A, Attachment I
Program Specifications

Part II – General

A. Additional Contract Restrictions

This Contract is subject to any additional restrictions, limitations, or conditions enacted by the Congress, or any statute enacted by the Congress, which may affect the provisions, terms, or funding of this Contract in any manner.

B. Hatch Act

Contractor agrees to comply with the provisions of the Hatch Act (Title 5 USC, Sections 1501-1508), which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

C. No Unlawful Use or Unlawful Use Messages Regarding Drugs

Contractor agrees that information produced through these funds, and which pertains to drugs and alcohol - related programs, shall contain a clearly written statement that there shall be no unlawful use of drugs or alcohol associated with the program. Additionally, no aspect of a drug or alcohol related program shall include any message on the responsible use, if the use is unlawful, of drugs or alcohol (HSC Section 11999-11999.3). By signing this Contract, Contractor agrees that it will enforce**,** and will require its subcontractors to enforce, these requirements.

D. Noncompliance with Reporting Requirements

Contractor agrees that DHCS has the right to withhold payments until Contractor has submitted any required data and reports to DHCS, as identified in Exhibit A, Attachment I, Part III - Reporting Requirements, or as identified in Document 1F(a), Reporting Requirements Matrix for Counties.

E. Limitation on Use of Funds for Promotion of Legalization of Controlled Substances

None of the funds made available through this Contract may be used for any activity that promotes the legalization of any drug or other substance included in Schedule I of Section 202 of the Controlled Substances Act (21 USC 812).

F. Debarment and Suspension

Contractor shall not subcontract with any party listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp. p. 189) and 12689 (3 CFR part 1989., p. 235), “Debarment and Suspension.” SAM exclusions contain the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

The Contractor shall advise all subcontractors of their obligation to comply with applicable federal debarment and suspension regulations, in addition to the requirements set forth in 42 CFR Part 1001.

Exhibit A, Attachment I
Program Specifications

G. Restriction on Distribution of Sterile Needles

No SABG funds made available through this Contract shall be used to carry out any program that includes the distribution of sterile needles or syringes for the hypodermic injection of any illegal drug unless DHCS chooses to implement a demonstration syringe services program for injecting drug users.

H. Health Insurance Portability and Accountability Act (HIPAA) of 1996

All work performed under this Contract is subject to HIPAA, Contractor shall perform the work in compliance with all applicable provisions of HIPAA. As identified in Exhibit F, DHCS and County shall cooperate to assure mutual agreement as to those transactions between them, to which this provision applies. Refer to Exhibit F for additional information.

1. Trading Partner Requirements

a) No Changes. Contractor hereby agrees that for the personal health information (Information), it will not change any definition, data condition or use of a data element or segment as proscribed in the Federal Health and Human Services (HHS) Transaction Standard Regulation (45 CFR 162.915 (a)).

b) No Additions. Contractor hereby agrees that for the Information, it will not add any data elements or segments to the maximum data set as proscribed in the HHS Transaction Standard Regulation (45 CFR 162.915 (b)).

c) No Unauthorized Uses. Contractor hereby agrees that for the Information, it will not use any code or data elements that either are marked “not used” in the HHS Transaction’s Implementation specification or are not in the HHS Transaction Standard’s implementation specifications (45 CFR 162.915 (c)).

d) No Changes to Meaning or Intent. Contractor hereby agrees that for the Information, it will not change the meaning or intent of any of the HHS Transaction Standard’s implementation specification (45 CFR 162.915 (d)).

2. Concurrence for Test Modifications to HHS Transaction Standards

Contractor agrees and understands that there exists the possibility that DHCS or others may request an extension from the uses of a standard in the HHS Transaction Standards. If this occurs, Contractor agrees that it will participate in such test modifications.

3. Adequate Testing

Contractor is responsible to adequately test all business rules appropriate to their types and specialties. If the Contractor is acting as a clearinghouse for enrolled providers, Contractor has obligations to adequately test all business rules appropriate to each and every provider type and specialty for which they provide clearinghouse services.

4. Deficiencies

   Contractor agrees to correct transactions, errors or deficiencies identified by DHCS, and transactions errors or deficiencies identified by an enrolled provider if the Contractor is acting as a clearinghouse for that provider. When County is a clearinghouse, Contractor agrees to properly communicate deficiencies and other pertinent information regarding electronic transactions to enrolled providers for which they provide clearinghouse services.

5. Code Set Retention

   Both parties understand and agree to keep open code sets being processed or used in this Contract for at least the current billing period or any appeal period, whichever is longer.

6. Data Transmission Log

   Both parties shall establish and maintain a Data Transmission Log which shall record any and all Data Transmissions taking place between the Parties during the term of this Contract. Each party will take necessary and reasonable steps to ensure that such Data Transmission Logs constitute a current, accurate, complete, and unaltered record of any and all Data Transmissions between the parties, and shall be retained by each Party for no less than twenty-four (24) months following the date of the Data Transmission. The Data Transmission Log may be maintained on computer media or other suitable means provided that, if it is necessary to do so, the information contained in the Data Transmission Log may be retrieved in a timely manner and presented in readable form.

I. Nondiscrimination and Institutional Safeguards for Religious Providers

Contractor shall establish such processes and procedures as necessary to comply with the provisions of Title 42, USC, Section 300x-65 and Title 42, CFR, Part 54, (Reference Document 1B).

J. Counselor Certification

Any counselor or registrant providing intake, assessment of need for services, treatment or recovery planning, individual or group counseling to participants, patients, or residents in a DHCS licensed or certified program is required to be registered or certified as defined in Title 9, CCR, Division 4, Chapter 8, (Document 3H).

K. Cultural and Linguistic Proficiency

To ensure equal access to quality care by diverse populations, each service provider receiving funds from this Contract shall adopt the Federal Office of Minority Health Culturally and Linguistically Appropriate Service (CLAS) national standards (Document 3V).

L. Intravenous Drug Use (IVDU) Treatment

Contractor shall ensure that individuals in need of IVDU treatment shall be encouraged to undergo AOD treatment (42 USC 300x-23 (45 CFR 96.126(e)).

Exhibit A, Attachment I
Program Specifications

M. Tuberculosis Treatment

Contractor shall ensure the following related to Tuberculosis (TB):

1. Routinely make available TB services to each individual receiving treatment for AOD use and/or abuse.

2. Reduce barriers to patients' accepting TB treatment.

3. Develop strategies to improve follow-up monitoring, particularly after patients leave treatment, by disseminating information through educational bulletins and technical assistance.

N. Trafficking Victims Protection Act of 2000

Contractor and its subcontractors that provide services covered by this Contract shall comply with the Trafficking Victims Protection Act of 2000 (22 United States Code (USC) 7104(g)) as amended by section 1702 of Pub. L. 112-239.

O. Tribal Communities and Organizations

Contractor shall regularly assess (e.g. review population information available through Census, compare to information obtained in the California Outcome Measurement System for Treatment (CalOMS-Tx) to determine whether the population is being reached, survey Tribal representatives for insight in potential barriers, the substance use service needs of the American Indian/Alaskan Native (AI/AN) population within the County geographic area, and shall engage in regular and meaningful consultation and collaboration with elected officials of the tribe, Rancheria, or their designee for the purpose of identifying issues/barriers to service delivery and improvement of the quality, effectiveness, and accessibility of services available to AI/NA communities within the County.

P. Participation of County Behavioral Health Director's Association of California.

The County AOD Program Administrator shall participate and represent the County in meetings of the County Behavioral Health Director's Association of California for the purposes of representing the counties in their relationship with DHCS with respect to policies, standards, and administration for AOD abuse services.

The County AOD Program Administrator shall attend any special meetings called by the Director of DHCS. Participation and representation shall also be provided by the County Behavioral Health Director's Association of California.

Q. Youth Treatment Guidelines

Contractor must comply with the guidelines in Document 1V, incorporated by this reference, "Youth Treatment Guidelines," in developing and implementing youth treatment programs funded under this Exhibit, until new Youth Treatment Guidelines are established and adopted. No formal amendment of this contract is required for new guidelines to be incorporated into this Contract.

Exhibit A, Attachment I
Program Specifications

R. Perinatal Services Network Guidelines

Contractor must comply with the perinatal program requirements as outlined in the Perinatal Services Network Guidelines. The Perinatal Services Network Guidelines are attached to this contract as Document 1G, incorporated by reference. The Contractor must comply with the current version of these guidelines until new Perinatal Services Network Guidelines are established and adopted. The incorporation of any new Perinatal Services Network Guidelines into this Contract shall not require a formal amendment.

Contractor receiving SABG funds must adhere to the Perinatal Services Network Guidelines, regardless of whether the Contractor exchanges perinatal funds for additional discretionary funds.

S. Byrd Anti-Lobbying Amendment (31 USC 1352)

Contractor certifies that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 USC 1352. Contractor shall also disclose to DHCS any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.

T. Nondiscrimination in Employment and Services

By signing this Contract, Contractor certifies that under the laws of the United States and the State of California, incorporated into this Contract by reference and made a part hereof as if set forth in full, Contractor will not unlawfully discriminate against any person.

U. Federal Law Requirements:

1. Title VI of the Civil Rights Act of 1964, Section 2000d, as amended, prohibiting discrimination based on race, color, or national origin in federally-funded programs.

2. Title VIII of the Civil Rights Act of 1968 (42 USC 3601 et seq.) prohibiting discrimination on the basis of race, color, religion, sex, handicap, familial status or national origin in the sale or rental of housing.

3. Age Discrimination Act of 1975 (45 CFR Part 90), as amended 42 USC Sections 6101 – 6107), which prohibits discrimination on the basis of age.

4. Age Discrimination in Employment Act (29 CFR Part 1625).

5. Title I of the Americans with Disabilities Act (29 CFR Part 1630) prohibiting discrimination against the disabled in employment.

6. Title II of the Americans with Disabilities Act (28 CFR Part 35) prohibiting discrimination against the disabled by public entities.

7. Title III of the Americans with Disabilities Act (28 CFR Part 36) regarding access.

8. Section 504 of the Rehabilitation Act of 1973, as amended (29 USC Section 794), prohibiting discrimination on the basis of individuals with disabilities.

9. Executive Order 11246 (42 USC 2000(e) et seq. and 41 CFR Part 60) regarding nondiscrimination in employment under federal contracts and construction contracts greater than $10,000 funded by federal financial assistance.

10. Executive Order 13166 (67 FR 41455) to improve access to federal services for those with limited English proficiency.

11. The Drug Abuse Office and Treatment Act of 1972, as amended, relating to nondiscrimination on the basis of drug abuse.

12. Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2, Subparts A – E).

V. State Law Requirements:

1. Fair Employment and Housing Act (Government Code Section 12900 et seq.) and the applicable regulations promulgated thereunder (2 CCR 7285.0 et seq.).

2. Title 2, Division 3, Article 9.5 of the Government Code, commencing with Section 11135.

3. Title 9, Division 4, Chapter 8 of the CCR, commencing with Section 13000.

4. No state or federal funds shall be used by the Contractor or its subcontractors for sectarian worship, instruction, or proselytization. No state funds shall be used by the Contractor or its subcontractors to provide direct, immediate, or substantial support to any religious activity.

5. Noncompliance with the requirements of nondiscrimination in services shall constitute grounds for DHCS to withhold payments under this Contract or terminate all, or any type, of funding provided hereunder.

W. Additional Contract Restrictions

1. This Contract is subject to any additional restrictions, limitations, or conditions enacted by the federal or state governments that affect the provisions, terms, or funding of this Contract in any manner.

X. Information Access for Individuals with Limited English Proficiency

1. Contractor shall comply with all applicable provisions of the Dymally-Alatorre Bilingual Services Act (Government Code sections 7290-7299.8) regarding access to materials that explain services available to the public as well as providing language interpretation services.

2. Contractor shall comply with the applicable provisions of Section 1557 of the Affordable Care Act (45 CFR Part 92), including, but not limited to, 45 CFR 92.201, when providing access to: (a) materials explaining services available to the public, (b) language assistance,

   (c) language interpreter and translation services, and (d) video remote language interpreting services.

Y. Subcontract Provisions

Contractor shall include all of the foregoing Part II general provisions in all of its subcontracts.

Exhibit A, Attachment I
Program Specifications

Part III – Reporting Requirements

Contractor agrees that DHCS has the right to withhold payments until Contractor has submitted any required data and reports to DHCS, as identified in this Exhibit A, Attachment I or as identified in Document 1F (a), Reporting Requirement Matrix for Counties.

A. Quarterly Federal Financial Management Report (QFFMR) - Quarterly Invoicing

Quarterly invoices serve as the Quarterly Federal Financial Management Report (QFFMR). The Contractor shall submit the QFFMR quarterly to reflect cumulative SABG expenditures.

For the beginning of each federal award year, the due dates are:

December 1 – 1st Quarterly Expenditures

March 1 – 1st and 2nd Quarterly Expenditures

June 1 – 1st, 2nd, and 3rd Cumulative Expenditures

September 1 – Total Fiscal Year Expenditures

B. California Outcomes Measurement System for Treatment (CalOMS-Tx)

The CalOMS-Tx business rules and requirements are:

1. Contractor shall internally comply with the CalOMS-Tx data collection system requirements for submission of CalOMS-Tx data or contract with a software vendor that does. If applicable, a Business Associate Agreement (BAA) shall be established between the Contractor and the software vendor, and the BAA shall state that DHCS is allowed to return the processed CalOMS-Tx data to the vendor that supplied the data to DHCS.

2. Contractor shall conduct information technology (IT) systems testing and pass State certification testing before commencing submission of CalOMS-Tx data. If the Contractor subcontracts with a vendor for IT services, Contractor is responsible for ensuring that the subcontracted IT system is tested and certified by the DHCS prior to submitting CalOMS-Tx data. If Contractor changes or modifies the CalOMS-Tx IT system, then Contractor shall re-test and pass state re-certification prior to submitting data from the new or modified system.

3. Electronic submission of CalOMS-Tx data shall be submitted by Contractor within 45 days from the end of the last day of the report month.

4. Contractor shall comply with data collection and reporting requirements established by the DHCS CalOMS-Tx Data Collection Guide (Document 3J) and all former Department of Alcohol and Drug Programs Bulletins and DHCS Information Notices relevant to CalOMS-Tx data collection.

5. Contractor shall submit CalOMS-Tx admission, discharge, annual update, resubmissions of records containing errors or in need of correction, and “provider no activity” report records in an electronic format approved by DHCS.

6. Contractor shall comply with the CalOMS-Tx Data Compliance Standards established by DHCS identified in Document 3S for reporting data content, data quality, data completeness, reporting frequency, reporting deadlines, and reporting method.

7. Contractor shall participate in CalOMS-Tx informational meetings, trainings, and conference calls. Contractor staff responsible for CalOMS-Tx data entry must have sufficient knowledge of the CalOMS-Tx Data Quality Standards, all new CalOMS-Tx users, whether employed by the Contractor or its subcontractors, shall participate in CalOMS-Tx trainings prior to inputting data into the system.

8. Contractor shall implement and maintain a system that complies with the CalOMS-Tx data collection system requirement for electronic submission of CalOMS-Tx data.

9. Contractor shall meet the requirements as identified in Exhibit F, Privacy and Information Security Provisions and Exhibit F, Attachment I - Social Security Administration Agreement.

C. Prevention Data Collection and Reporting Service

The Prevention Data Collection and Reporting Service business rules and requirements are:

1. Contractors and/or subcontractors receiving SABG Primary Prevention Set-Aside funding shall input planning, service/activity and evaluation data into the service. When submitting data, Contractor shall comply with the Prevention Data Quality Standards (Document #1T).

2. Contractor shall report services/activities by the date of occurrence on an ongoing basis throughout each month. Contractor shall submit all data for each month no later than the 10th day of the following month.

3. Contractor shall review all data input into the prevention data collection service on a quarterly basis. Contractor shall verify that the data meets the Prevention Data Quality Standards. Certification is due by the last day of the month following the end of the quarter.

4. Contractor shall report progress to DHCS on the goals and objectives in the County SPP (as described in Exhibit A, Attachment I, Part I, Section 2 (B) (2)) on an annual basis by September 30th of each fiscal year.

5. If Contractor cannot meet the established due dates, a written request for an extension shall be submitted to DHCS 10 calendar days prior to the due date.

6. In order to ensure that all persons responsible for prevention data entry have sufficient knowledge of the Prevention Data Quality Standards, all new users of the service, whether employed by the Contractor or its subcontractors, shall participate in prevention data collection and reporting training prior to inputting any data.

D. CalOMS-Tx and Prevention Data Collection and Reporting General Information

1. If the Contractor experiences system or service failure or other extraordinary circumstances that affect its ability to timely submit CalOMS-Tx and/or prevention data, and or meet other CalOMS-Tx and/or prevention data compliance requirements, Contractor shall report the problem in writing by secure, encrypted e-mail to DHCS by e-mail at:

ITServiceDesk@dhcs.ca.gov before the established data submission deadlines. The written notice shall include a remediation plan that is subject to review and approval by DHCS. A grace period of up to 60 days may be granted, at the State's sole discretion, for the Contractor to resolve the problem before SABG payments are withheld.

2. If DHCS experiences system or service failure, no penalties will be assessed to the Contractor for late data submission.

3. Contractor shall comply with the treatment and prevention data quality standards established by DHCS. Failure to meet these standards on an ongoing basis may result in withholding SABG funds.

4. If the Contractor submits data after the established deadlines, due to a delay or problem, Contractor is still responsible for collecting and reporting data from time of delay or problem.

E. Drug and Alcohol Treatment Access Report (DATAR)

The DATAR business rules and requirements are:

1. The Contractor shall be responsible for ensuring that the Contractor-operated treatment services and all treatment providers, with whom Contractor makes a contract or otherwise pays for the services, submit a monthly DATAR report in an electronic copy format as provided by DHCS.

   In those instances, where the Contractor maintains, either directly or indirectly, a central intake unit or equivalent which provides intake services including a waiting list, the Contractor shall identify and begin submitting monthly DATAR reports for the central intake unit by a date to be specified by DHCS.

2. The Contractor shall ensure that all DATAR reports are submitted by either Contractor-operated treatment services and by each subcontracted treatment provider to DHCS by the 10th of the month following the report activity month.

3. The Contractor shall ensure that all applicable providers are enrolled in DHCS' web-based DATARWeb program for submission of data, accessible on the DHCS website when executing the subcontract.

4. If the Contractor or its subcontractor experiences system or service failure or other extraordinary circumstances that affect its ability to timely submit a monthly DATAR report, and/or to meet data compliance requirements, the Contractor shall report the problem in writing by secure, encrypted e-mail to: DHCS by e-mail at ITServiceDesk@dhcs.ca.gov before the established data submission deadlines. The written notice shall include a corrective action plan that is subject to review and approval by DHCS. A grace period of up to 60 days may be granted, at DHCS' sole discretion, for the Contractor to resolve the problem before SABG payments are withheld pursuant to 45 CFR Section 75.371 and HSC Section 11817.8. (See Exhibit B, Part II, Section (2)(A)(6)).

5. If DHCS experiences system or service failure, no penalties will be assessed to Contractor for late data submission.

6. The Contractor shall be considered compliant if a minimum of 95% of required DATAR reports from the Contractor's treatment providers are received by the due date.

F. Charitable Choice

Contractor shall document the total number of referrals necessitated by religious objection to other alternative SUD providers. The Contractor shall annually submit this information to DHCS' Program Support and Grants Management Branch by e-mail at DHCSSUDCharitableChoice@dhcs.ca.gov by October 1st. The annual submission shall contain all substantive information required by DHCS and be formatted in a manner prescribed by DHCS.

G. Subcontractor Documentation

Contractor shall require its subcontractors that are not licensed or certified by DHCS to complete and submit non-drug Medi-Cal organizational forms within 30 days of the execution of an initial subcontract, within 90 days of the renewal or continuation of an existing subcontract or when there has been a change in subcontractor name or ownership. Non-Drug Medi-Cal Organizational forms shall be submitted through http://www.dhcs.ca.gov/provgovpart/Pages/Master-Provider-File-Database-Resources.aspx. Organizational documents shall include the subcontractor's Articles of Incorporation or Partnership Agreements (as applicable), business licenses, fictitious name permits, and such other information and documentation as may be requested by DHCS.

H. Failure to meet required reporting requirements shall result in:

1. DHCS will issue a Notice of Deficiency (Deficiencies) to Contractor regarding specified providers with a deadline to submit the required data and a request for a CAP to ensure timely reporting in the future. DHCS will approve or reject the CAP or request revisions to the CAP, which shall be resubmitted to the DHCS within 30 days.

2. If the Contractor has not ensured compliance with the data submission or CAP request within the designated timeline, then DHCS shall withhold funds until all data is submitted. DHCS shall inform the Contractor when funds will be withheld.

Exhibit A, Attachment I
Program Specifications

Part IV – Definitions

Section 1 - General Definitions

The words and terms of this Contract are intended to have their usual meanings unless a particular or more limited meaning is associated with their usage pursuant to Division 10.5 of HSC, Section 11750 et seq., and Title 9, CCR, Section 9000 et seq.

A. **"Available Capacity"** means the total number of units of service (bed days, hours, slots, etc.) that a Contractor actually makes available in the current fiscal year.

B. **"Contractor"** means the county identified in the Standard Agreement or the department authorized by the County Board of Supervisors to administer substance use disorder programs.

C. **"Corrective Action Plan (CAP)"** means the written plan of action document which the Contractor or its subcontracted service provider develops and submits to DHCS to address or correct a deficiency or process that is non-compliant with laws, regulations or standards.

D. **"County"** means the county in which the Contractor physically provides covered substance use treatment services.

E. **"Days"** means calendar days, unless otherwise specified.

F. **"Dedicated Capacity"** means the historically calculated service capacity, by modality, adjusted for the projected expansion or reduction in services, which the Contractor agrees to make available to provide SABG services to persons eligible for Contractor's services.

G. **"First-Tier Sub-recipient"** means the "Contractor" identified in the Standard Agreement or the department authorized by the County Board of Supervisors to administer substance use disorder programs funded by the SABG.

H. **"Final Allocation"** means the amount of funds identified in the last allocation letter issued by DHCS for the current fiscal year.

I. **"Final Settlement"** means permanent settlement of the Contractor's actual allowable costs or expenditures as determined at the time of audit, which shall be completed within three years of the date the year-end cost settlement report was accepted for interim settlement by DHCS. If the audit is not completed within three years, the interim settlement shall be considered as the final settlement.

J. **"Interim Settlement"** means temporary settlement of actual allowable costs or expenditures reflected in the Contractor's year-end cost settlement report.

K. **"Key points of contact"** means common points of access to substance use treatment services from the county, including but not limited to the county's beneficiary problem resolution process, county owned or operated or contract hospitals, and any other central access locations established by the county.

L. **"Maximum Payable"** means the encumbered amount reflected on the Standard Agreement of this Contract and supported by Exhibit B, Attachment I.

Exhibit A, Attachment I
Program Specifications

M. "Modality" means those necessary overall general service activities to provide substance use disorder services as described in Division 10.5 of the HSC.

N. "SABG Amount" means the contracted amount of SABG funds for services agreed to by DHCS and the Contractor.

O. "Performance" means providing the dedicated capacity in accordance with Exhibit B, Attachment I, and abiding by the terms of this Exhibit, including all applicable state and federal statutes, regulations, and standards, including Alcohol and/or Other Drug Certification Standards (Document 1P), in expending funds for the provision of substance use disorder services hereunder.

P. "Preliminary Settlement" means the settlement of only SABG funding for counties that do include DMC funding.

Q. "Revenue" means Contractor's income from sources other than DHCS allocation.

R. "Second-Tier Subrecipient" means an entity that has entered into an agreement with the Contractor to be a provider of substance use disorder services funded by the SABG.

S. "Service Area" means the geographical area under Contractor's jurisdiction.

T. "Service Element" is the specific type of service performed within the more general service modalities. A list of the service modalities and service elements and service elements codes is incorporated into this Contract as Document 1H(a) "Service Code Descriptions".

U. "State" means the Department of Health Care Services or DHCS.

V. "Sub-recipient Pre-Award Risk Assessment" means the Contractor's responsibility to review the merit and risk associated with all potential grant recipients prior to making an award as described in 2 CFR Part 200 Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, commonly referred to as the Uniform Guidance.

W. "Utilization" means the total actual units of service used by clients and participants further defined as the count of persons with initial admissions and subsequent admission(s) to an episode of care.

Exhibit A, Attachment I
Program Specifications

DOCUMENTS INCORPORATED BY REFERENCE

The following documents are hereby incorporated by reference into the County contract though they may not be physically attached to the contract but will be issued in a CD under separate cover:

Document 1A:	Title 45, Code of Federal Regulations 96, Subparts C and L, Substance Abuse Prevention and Treatment Block Grant Requirements https://www.gpo.gov/fdsys/granule/CFR-2005-title45-vol1/CFR-2005-title45-vol1-part96
Document 1B:	Title 42, Code of Federal Regulations, Charitable Choice Regulations https://www.law.cornell.edu/cfr/text/42/part-54
Document 1C:	Driving-Under-the-Influence Program Requirements
Document 1F(a):	Reporting Requirement Matrix - County Submission Requirements for the Department of Health Care Services
Document 1G:	Perinatal Services Network Guidelines 2016-17 http://www.dhcs.ca.gov/services/adp/Documents/psng%20FY%202016-17.pdf
Document 1K:	Drug and Alcohol Treatment Access Report (DATAR) User Manual http://www.dhcs.ca.gov/provgovpart/Pages/DATAR.aspx
Document 1N:	Guide to Writing a Strategic Prevention Plan
Document 1O:	Strategic Prevention Plan Workbook for Counties
Document 1P:	Alcohol and/or Other Drug Program Certification Standards (May 1, 2017) http://www.dhcs.ca.gov/Documents/DHCS_AOD_Certification_Standards.pdf
Document 1T :	CalOMS Prevention Data Quality Standards
Document 1V:	Youth Treatment Guidelines http://www.dhcs.ca.gov/individuals/Documents/Youth_Treatment_Guidelines.pdf
Document 2F(b):	Minimum Quality Drug Treatment Standards for SABG
Document 2P:	County Certification - Cost Report Year-End Claim For Reimbursement

Exhibit A, Attachment I
Program Specifications

Document 3G:	California Code of Regulations, Title 9 - Rehabilitation and Developmental Services, Division 4 - Department of Alcohol and Drug Programs, Chapter 4 - Narcotic Treatment Programs http://www.calregs.com
Document 3H:	California Code of Regulations, Title 9 - Rehabilitation and Developmental Services, Division 4 - Department of Alcohol and Drug Programs, Chapter 8 - Certification of Alcohol and Other Drug Counselors http://www.calregs.com
Document 3J:	CalOMS Treatment Data Collection Guide http://www.dhcs.ca.gov/provgovpart/Documents/CalOMS_Tx_Data_Collection_Guide_JAN%202014.pdf
Document 3O:	Quarterly Federal Financial Management Report (QFFMR) http://www.dhcs.ca.gov/provgovpart/Pages/SUD_Forms.aspx
Document 3S:	CalOMS Treatment Data Compliance Standards http://www.dhcs.ca.gov/provgovpart/Documents/CalOMS_data_cmpliance%20standards%202014.pdf
Document 3T:	Non-Drug Medi-Cal and Drug Medi-Cal DHCS Local Assistance Funding Matrix
Document 3T(a):	SAPT Authorized and Restricted Expenditures Information (April 2017)
Document 3V :	Culturally and Linguistically Appropriate Services (CLAS) National Standards https://www.minorityhealth.hhs.gov/omh/browse.aspx?lvl=2&lvlid=53
Document 5A :	Confidentiality Agreement

Exhibit B
Budget Detail and Payment Provisions

Part I – General Fiscal Provisions

Section 1 – General Fiscal Provisions

A. Fiscal Provisions

For services satisfactorily rendered, and upon receipt and approval of documentation as identified in Exhibit A, Attachment I, Part III, the Department of Health Care Services (DHCS) agrees to compensate the Contractor for actual expenditures incurred in accordance with the rates and/or allowable costs specified herein.

B. Funding Authorization

Contractor shall bear the financial risk in providing any substance use disorder services covered by this Contract.

C. Availability of Funds

It is understood that, for the mutual benefit of both parties, this Contract may have been written before ascertaining the availability of congressional appropriation of funds in order to avoid program and fiscal delays that would occur if this Contract were not executed until after that determination. If so, DHCS may amend the amount of funding provided for in this Contract based on the actual congressional appropriation.

D. Budget Contingency Clause

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

If the funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, DHCS shall solely have the option to either cancel this Contract with no liability occurring to DHCS, or offer an amended agreement to Contractor to reflect the reduced amount.

E. Expense Allowability / Fiscal Documentation

1. Invoices, received from a Contractor and accepted and/or submitted for payment by DHCS, shall not be deemed evidence of allowable agreement costs.

2. Contractor shall maintain for review, audit, and supply to DHCS upon request, adequate documentation of all expenses claimed pursuant to this Contract to permit a determination of expense allowability.

3. If the allowability or appropriateness of an expense cannot be determined by DHCS because invoice detail, fiscal records, or backup documentation is nonexistent or inadequate according to generally accepted accounting principles, and generally accepted governmental audit standards, all questionable costs may be disallowed and payment may

be withheld by DHCS. Upon receipt of adequate documentation supporting a disallowed or questionable expense, reimbursement may resume for the amount substantiated and deemed allowable.

4. Costs and/or expenses deemed unallowable shall not be reimbursed or, if mistakenly reimbursed, those costs and/or expenses shall be subject to recovery by DHCS pursuant to HSC Code 11817.8(e).

F. Maintenance of Effort for the Substance Abuse Prevention and Treatment Block Grant

1. Notwithstanding any other provision in this Contract, the Director of DHCS may reduce federal funding allocations, on a dollar-for-dollar basis, to a county that has a reduced or anticipates reduced expenditures in a way that would result in a decrease in California's receipt of Federal Substance Abuse Prevention and Treatment Block Grant (SABG) funds (42 United States Code (U.S.C.) Sect 300x-30).

2. Prior to making any reductions pursuant to this subdivision, the Director shall notify all counties that county underspending will reduce the Federal SABG Maintenance Of Effort (MOE). Upon receipt of notification, a county may submit a revision to the county budget initially submitted pursuant to HSC Section 11798 subdivision(a) in an effort to maintain the statewide SABG MOE.

3. Pursuant to HSC Section 11814(d)(3), a county shall notify DHCS in writing of proposed local changes to the county's expenditure of funds. DHCS shall review and may approve the proposed local changes depending on the level of expenditures needed to maintain DHCS wide SABG MOE.

G. SABG Primary Prevention Services Expenditure Requirement

Pursuant to Title 42, U.S.C. Section 300x-22(a), the Contractor shall expend a minimum of 20 percent of SABG funds for primary prevention services. The Contractor shall expend primary prevention funds for strategies, programs and services directed at individuals who have not been determined to require treatment for a substance use disorder. These programs shall educate and counsel individuals on substance abuse and provide for activities to reduce the risk of such abuse by the individuals. The Contractor shall give priority to programs for populations that are at risk of developing a pattern of substance abuse and ensure that those programs develop community-based prevention strategies.

H. SABG Women Services Expenditure Requirement

Pursuant to Title 42, U.S.C. 5 Section 300x-22(b) and 45 Code of Federal Regulations (CFR) 96.124(c), for each state fiscal year (SFY) the Contractor shall expend an amount of SABG funds not less than the amount expended by the Contractor in fiscal year 1994 on perinatal services, pregnant women, and women with dependent children. The Contractor shall expend that percentage either by establishing new programs or expanding the capacity of existing programs in the manner described in Exhibit G of the annual SABG allocation, "County Share of SABG Women Services Expenditure Requirements" (found at http://www.dhcs.ca.gov/formsandpubs/Documents/Info%20Notice%202015/11-Exhibit_G.pdf).

Exhibit B
Budget Detail and Payment Provisions

Section 2 – General Fiscal Provisions – SABG

A. Revenue Collection

Contractor shall conform to revenue collection requirements in HSC Sections 11841, by raising revenues in addition to the funds allocated by DHCS. These revenues include, but are not limited to, fees for services, private contributions, grants, or other governmental funds. These revenues shall be used in support of additional alcohol and other drug services or facilities. Each alcohol and drug program shall set and collect client fees based on the client's ability to pay. The fee requirement shall not apply to prevention and early intervention services. Contractor shall identify in its annual cost report the types and amounts of revenues collected.

B. Cost Efficiencies

It is intended that the cost to the Contractor in maintaining the dedicated capacity and units of service shall be met by the SABG funds allocated to the Contractor and other Contractor or subcontractor revenues. Amounts awarded pursuant to Exhibit A, Attachment I, Part I, shall not be used for services where payment has been made, or can reasonably be expected to be made under any other state or federal compensation or benefits program, or where services can be paid for from revenues.

Exhibit B
Budget Detail and Payment Provisions

Part II – Reimbursements

Section 1 - General Reimbursement

A. Prompt Payment Clause

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

B. Amounts Payable

1. The amount payable under this Contract shall not exceed the amount identified on the State of California Standard Agreement form STD 213 DHCS.

2. Reimbursement shall be made for allowable expenses up to the amount annually encumbered commensurate with the state fiscal year in which services are performed and/or goods are received.

3. The funds identified for the fiscal years covered by this Section, within this Exhibit, are subject to change depending on the availability and amount of funds appropriated by the Legislature and the Federal Government. The amount of funds available for expenditure by the Contractor shall be limited to the amount identified in the final allocations issued by DHCS for that fiscal year or the SABG amount, whichever is less. Changes to allocated funds will require a written amendment to the Contract.

4. For each fiscal year, DHCS may settle costs for services based on the year-end cost settlement report. The year-end cost settlement shall be the final amendment for the state fiscal year.

Section 2 - Substance Abuse Prevention and Treatment Block Grant (SABG)

A. Amounts Payable for SABG

1. DHCS shall reimburse the Contractor monthly in arrears an amount equal to one-twelfth of the maximum amount allowed pursuant to Exhibit B of the Contract or the most recent allocation based on the Budget Act Allocation, whichever is less. Final allocations will reflect any increases or reductions in the appropriations as reflected in DHCS Budget Act allocation and any subsequent allocation revisions.

2. Quarterly Invoicing-Quarterly Federal Financial Management Report (QFFMR)

   a) Chapter 8760 of the State Administrative Manual requires DHCS to establish control mechanisms to ensure that the Contractor does not spend beyond its allocation and that DHCS does not reimburse beyond the Contractor's allocation. The Contractor shall complete quarterly invoices as prescribed by DHCS that serve as expenditure reports during the fiscal year. The Contractor shall incur expenditures before receiving payment from its allocation. These expenditures are documented as totals in aggregate.

Exhibit B
Budget Detail and Payment Provisions

Quarterly invoices are due:

- December 1-1st Quarter
- March 1-2nd Quarter
- June 1-3rd Quarter
- September 1-4th Quarter

These invoices serve as payment authorizations. Payment authorizations are analyzed by DHCS to ensure that costs are reasonable and do not exceed the Contractor's allocation. Inaccuracies in the report shall be resolved by the Contractor prior to receiving payment. These quarterly invoices serve as the Quarterly Federal Financial Management Report (QFFMR).

3. Monthly disbursements to the Contractor at the beginning of each fiscal year of the Contract shall be based on the preliminary allocation of funds, as detailed in Section 2 of this Exhibit.

4. Based on the expenditure information submitted by the counties in the QFFMR (Document 3O), DHCS may adjust monthly payments of encumbered block grant federal funds to extend the length of time (not to exceed 21 months) over which payments of federal funds will be made.

5. Pursuant to 45 CFR Section 75.371 and HSC Section 11817.8, DHCS may withhold monthly SABG payments if the Contractor fails to:

   a) Submit timely reports and data required by DHCS, including but not limited to, reports required pursuant to Exhibit A, Attachment I, Part III.

   b) Submit a Contract amendment within 90 days from issuance from DHCS to the Contractor.

   c) Submit monitoring reports and attest the completion of Corrective Action Plans (CAP) for services provided pursuant to this Contract.

   d) Monitor its subcontractors annually pursuant to Exhibit A, Attachment I, Part I.

6. In the event DHCS withholds SABG payment, the Contractor's payment shall commence with the next scheduled monthly payment following DHCS' receipt and acceptance of complete and accurate reports, data, or executed Contract. The payment shall include any funds withheld pursuant to Section 2(A)(5).

7. Adjustments may be made to the total Contract amount and funds may be withheld from payments otherwise due to the Contractor hereunder, for nonperformance to the extent that nonperformance involves fraud, abuse, or failure to achieve the objectives of the provisions of Exhibit A, Attachment I, Part I.

B. Payment Provisions

For each fiscal year, the total amount payable by DHCS to the Contractor for services provided under Exhibit A, Attachment I, Part I, shall not exceed the encumbered amount. The funds

identified for the fiscal years covered by Exhibit A, Attachment I, Part I, are subject to change depending on the availability and amount of funds appropriated by the Legislature and the Federal Government. Changes to encumbered funds require a written amendment to the Contract. DHCS may settle costs for SABG services based on the year-end cost settlement report as the final amendment to the approved single state/county Contract.

C. In the event of a Contract amendment, as required by the preceding paragraph, the Contactor shall submit to DHCS the information identified in Exhibit E, Section (1)(B). To the extent the Contractor is notified of the State Budget Act allocation prior to the execution of the Contract, DHCS and the Contractor may agree to amend the Contract after the issuance of the first Budget Act allocation.

D. Accrual of Interest

Any interest accrued from state-allocated funds and retained by the Contractor shall be used for the same purpose as DHCS allocated funds from which the interest was accrued.

E. Expenditure Period

SABG funds are allocated based upon the Federal Grant award period. These funds must be expended for activities authorized pursuant to 42 USC Sections 300x-21 through 300x-66, and Title 45 CFR 96.120 et seq., within the availability period of the grant award. Any SABG funds that have not been expended by the Contractor at the end of the expenditure period identified below shall be returned to DHCS for subsequent return to the Federal Government.

1. The expenditure period of the FFY 2015 award is October 1, 2015 through June 30, 2017.

2. The expenditure period of the FFY 2016 award is October 1, 2016 through June 30, 2018.

3. The expenditure period of the FFY 2017 award is October 1, 2017 through June 30, 2019.

4. The expenditure period of the FFY 2018 award is October 1, 2018 through June 30, 2020.

5. The expenditure period of the FFY 2019 award is October 1, 2019 through June 30, 2021.

F. Contractors receiving SABG funds shall comply with the financial management standards contained in 45 CFR Sections 75.302(b)(1) through (6), and 45 CFR Section 96.30.

G. Non-profit subcontractors receiving SABG funds shall comply with the financial management standards contained in 45 CFR Section 75.302(b)(1) through (4) and (b)(7), and 45 CFR Section 96.30.

H. Contractors receiving SABG funds shall track obligations and expenditures by individual SABG award, including, but not limited to, obligations and expenditures for primary prevention, services to pregnant women and women with dependent children. “Obligation” shall have the same meaning as used in 45 CFR Section 75.2.

Exhibit B
Budget Detail and Payment Provisions

I. Restrictions on the Use of SABG Funds

Pursuant to 42 USC 300x-31, Contractor shall not use SABG funds provided by the Contract on the following activities:

1. Provide inpatient services.

2. Make cash payment to intended recipients of health services.

3. Purchase or improve land, purchase, construct or permanently improve (other than minor remodeling) any building or other facility or purchase major medical equipment.

4. Satisfy any requirement for the expenditure of SABG funds as a condition for the receipt of federal funds.

5. Provide financial assistance to any entity other than a public or nonprofit private entity.

6. Pay the salary of an individual through a grant or other extramural mechanism at a rate in excess of level I of the Executive Salary Schedule for the award year: see http://grants.nih.gov/grants/policy/salcap_summary.htm.

7. Purchase treatment services in penal or correctional institutions of this State of California.

8. Supplant state funding of programs to prevent and treat substance abuse and related activities.

9. Carry out any program prohibited by 42 USC 300x–21 and 42 USC 300ee–5 such that none of the funds provided under this Act or an amendment made by this Act shall be used to provide individuals with hypodermic needles or syringes so that such individuals may use illegal drugs, unless the Surgeon General of the United States Public Health Service determines that a demonstration needle exchange program would be effective in reducing drug abuse and the risk that the public will become infected with the etiologic agent for acquired immune deficiency syndrome.

10. Exception regarding inpatient hospital services:

    a) Medical necessity as precondition: With respect to compliance with the agreement made under this Exhibit, Part II, Section 2(I), a State may expend a grant under 42 USC 300x–21 to provide inpatient hospital services as treatment for substance abuse only if it has been determined, in accordance with guidelines issued by the Secretary, that such treatment is a medical necessity for the individual involved, and that the individual cannot be effectively treated in a community-based, nonhospital, residential program of treatment.

    b) Rate of payment: In the case of an individual for whom a grant under section 300x–21 of this title is expended to provide inpatient hospital services described in paragraph (1), a funding agreement for the grant for the State involved is that the daily rate of payment provided to the hospital for providing the services to the individual will not exceed the comparable daily rate provided for community-based, non-hospital, residential programs of treatment for substance abuse.

Exhibit B
Budget Detail and Payment Provisions

11. Waiver regarding construction of facilities:

    a) In general: The Secretary may provide to any State a waiver of the restriction established in 42 USC 300x–31, subsection (a)(1)(C), for the purpose of authorizing DHCS to expend a grant under section 42 USC 300x–21 for the construction of a new facility or rehabilitation of an existing facility, but not for land acquisition.

    b) Standard regarding need for waiver: The Secretary may approve a waiver under 42 USC 300x–31 (c), only if DHCS demonstrates to the Secretary that adequate treatment cannot be provided through the use of existing facilities and that alternative facilities in existing suitable buildings are not available.

    c) Amount: In granting a waiver under 42 USC 300x–31 (c), the Secretary shall allow the use of a specified amount of funds to construct or rehabilitate a specified number of beds for residential treatment and a specified number of slots for outpatient treatment, based on reasonable estimates by DHCS of the costs of construction or rehabilitation. In considering waiver applications, the Secretary shall ensure that DHCS has carefully designed a program that will minimize the costs of additional beds.

    d) Matching funds: The Secretary may grant a waiver under 42 USC 300x–31 (c), only if DHCS agrees, with respect to the costs to be incurred by DHCS in carrying out the purpose of the waiver, to make available non-federal contributions in cash toward such costs in an amount equal to not less than $1 for each $1 of federal funds provided under 42 USC 300x–21.

    e) Date certain for acting upon request: The Secretary shall act upon a request for a waiver under 42 USC 300x–31 (c), not later than 120 days after the date on which the request is made.

Exhibit B
Budget Detail and Payment Provisions

Part III - Financial Audit Requirements

Section 1 - General Fiscal Audit Requirements

A. In addition to the requirements identified below, the Contractor and its subcontractors are required to meet the audit requirements as delineated in Exhibit C, General Terms and Conditions, and Exhibit D(F), Special Terms and Conditions, of this Contract.

B. All expenditures of county realignment funds, state and federal funds furnished to the Contractor and its subcontractors pursuant to this Contract are subject to audit by DHCS. Such audits shall consider and build upon external independent audits performed pursuant to audit requirements of 45 CFR, Part 75, Subpart F and/or any independent Contractor audits or reviews. Objectives of such audits may include, but are not limited to, the following:

1. To determine whether units of service claimed/reported are properly documented by service records and accurately accumulated for claiming/reporting.

2. To validate data reported by the Contractor for prospective contract negotiations.

3. To provide technical assistance in addressing current year activities and providing recommendations on internal controls, accounting procedures, financial records, and compliance with laws and regulations.

4. To determine the cost of services, net of related patient and participant fees, third party payments, and other related revenues and funds.

5. To determine that expenditures are made in accordance with applicable state and federal laws and regulations and contract requirements.

6. To determine the facts in relation to analysis of data, complaints, or allegations, which may be indicative of fraud, abuse, willful misrepresentation, or failure to achieve the Contract objectives.

C. Unannounced visits to the Contractor and/or its subcontractors may be made at the discretion of DHCS.

D. The refusal of the Contractor or its subcontractors to permit access to and inspection of electronic or print books and records, physical facilities, and/or refusal to permit interviews with employees, as described in this part constitutes an express and immediate material breach of this Contract and will be sufficient basis to terminate the Contract for cause or default.

E. Reports of audits conducted by DHCS shall reflect all findings, recommendations, adjustments and corrective actions as a result of its finding in any areas.

Section 2. SABG Financial Audits

A. Contractor shall monitor the activities of all of its subcontractors to ensure that the SABG funds are used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the grant and that performance goals are achieved.

Exhibit B
Budget Detail and Payment Provisions

B. Contractor may use a variety of monitoring mechanisms, including limited scope audits, on-site visits, progress reports, financial reports, and review of documentation support requests for reimbursement, to meet the Contractor's monitoring objectives. Contractor may charge federal awards for the cost of these monitoring procedures if permitted under 45 CFR 75.425.

C. Contractor shall submit to DHCS a copy of the procedures and any other monitoring mechanism used to monitor non-profit Subcontracts at the time of the County's annual desk review or site visit or within 60 days thereafter. Contractor shall state the frequency that non-profit Subcontracts are monitored.

D. On-site visits focus on compliance and controls over compliance areas. The DHCS County Monitoring Unit analyst shall make site visits to the subcontractor locations(s), and can use a variety of monitoring mechanisms to document compliance requirements. The Contractor shall follow-up on any findings and the corrective actions. 42 USC 300x–31 subsection (a)(1)(C)

    1. Contractor shall be responsible for any disallowance taken by the Federal Government, DHCS, or the California State Auditor, as a result of any audit exception that is related to the Contractor's responsibilities herein. Contractor shall not use funds administered by DHCS to repay one federal funding source with funds provided by another federal funding source, to repay federal funds with state funds, or to repay state funds with federal funds. DHCS shall invoice Contractor 60 days after issuing the final audit report or upon resolution of an audit appeal. Contractor agrees to develop and implement any CAP in a manner acceptable to DHCS in order to comply with recommendations contained in any audit report. Such CAP plans shall include time-specific objectives to allow for measurement of progress and are subject to verification by DHCS within one year from the date of the plan.

E. Contractors that conduct financial audits of subcontractors, other than a subcontractor whose funding consists entirely of non-Department funds, shall develop a process to resolve disputed financial findings and notify subcontractors of their appeal rights pursuant to that process. If any fiscal adjustments remain after the Contractor and subcontractor have exhausted the internal appeals process, any SABG funds outstanding shall be returned to DHCS. This section shall not apply to those grievances or compliances arising from the financial findings of an audit or examination made by or on behalf of DHCS pursuant to Part III of this Exhibit.

F. If the Contractor fails to comply with Federal statues, regulations, or the terms and conditions of the grant, DHCS may impose additional conditions on the subaward, including:

    1. Requiring additional or more detailed financial reports.

    2. Requiring technical or management assistance.

    3. Establishing additional prior approvals.

G. If DHCS determines that the Contractor's noncompliance cannot be remedied by imposing additional conditions, DHCS may take one or more of the following actions:

    a. Temporarily withhold cash payment pending correction of the deficiency by the Contractor.

    b. Disallow all or part of the cost of the activity or action not in compliance.

c. Wholly or partly suspend the award activities or terminate the Contractor's subaward.

d. Recommend that the suspension or debarment proceedings be initiated by the Federal awarding agency.

e. Withhold further Federal awards.

f. Take other remedies that may be legally available.

Exhibit B
Budget Detail and Payment Provisions

Part IV – Records

Section 1 - General Provisions

A. Maintenance of Records

Contractor shall maintain sufficient books, records, documents, and other evidence necessary for DHCS to audit contract performance and contract compliance. Contractor shall make these records available to SAMHSA, Inspectors General, the Comptroller General, DHCS, or any of their authorized representatives upon request, to evaluate the quality and quantity of services, accessibility and appropriateness of services, and to ensure fiscal accountability. Regardless of the location or ownership of such records, they shall be sufficient to determine if costs incurred by Contractor are reasonable, allowable and allocated appropriately. All records must be capable of verification by qualified auditors.

1. Contractor and subcontractors shall include in any contract with an audit firm a clause to permit access by DHCS to the working papers of the external independent auditor, and require that copies of the working papers shall be made for DHCS at its request.

2. Contractor and subcontractors shall keep adequate and sufficient financial records and statistical data to support the year-end documents filed with DHCS. All records must be capable of verification by qualified auditors.

3. Accounting records and supporting documents shall be retained for a three-year period from the date the year-end cost settlement report was approved by DHCS for interim settlement. When an audit by the Federal Government, DHCS, or the California State Auditor has been started before the expiration of the three-year period, the records shall be retained until completion of the audit and final resolution of all issues that arise in the audit. Final settlement shall be made at the end of the audit and appeal process. If an audit has not been completed within three years, the interim settlement shall be considered as the final settlement.

4. Financial records shall be kept so that they clearly reflect the source of funding for each type of service for which reimbursement is claimed. These documents include, but are not limited to, all ledgers, books, vouchers, time sheets, payrolls, appointment schedules, client data cards, and schedules for allocating costs. All records must be capable of verification by qualified auditors.

5. Contractor's subcontracts shall require that all subcontractors comply with the requirements of Exhibit A, Attachment I, Part I, Section 3.

6. Should a subcontractor discontinue its contractual agreement with the Contractor, or cease to conduct business in its entirety, Contractor shall be responsible for retaining the subcontractor's fiscal and program records for the required retention period. The State Administrative Manual (SAM) contains statutory requirements governing the retention, storage, and disposal of records pertaining to state funds. Contractor shall follow SAM requirements located at http://sam.dgs.ca.gov/TOC/1600.aspx.

7. The Contractor shall retain all records in accordance with the time periods outlined in 45 CFR Section 75.361.

8. In the expenditure of funds hereunder, and as required by 45 CFR Part 96, Contractor shall comply with the requirements of SAM and the laws and procedures applicable to the obligation and expenditure of federal and state funds.

B. Dispute Resolution Process

1. In the event of a dispute under this Exhibit A, Attachment I, Part I, other than an audit dispute, Contractor shall provide written notice of the particulars of the dispute to DHCS before exercising any other available remedy. Written notice shall include the contract number. The Director (or designee) of DHCS and the County Drug or Alcohol Program Administrator (or designee) shall meet to discuss the means by which they can effect an equitable resolution to the dispute. Contractor shall receive a written response from DHCS within 60 days of the notice of dispute. The written response shall reflect the issues discussed at the meeting and state how the dispute will be resolved.

2. Contractors that conduct financial audits of subcontractors, other than a subcontractor whose funding consists entirely of non-Department funds, shall develop a process to resolve disputed financial findings and notify subcontractors of their appeal rights pursuant to that process. If any fiscal adjustments remain after the Contractor and subcontractor have exhausted the internal appeals process, any SABG funds outstanding must be returned to DHCS. This section shall not apply to those grievances or compliances arising from the financial findings of an audit or examination made by or on behalf of DHCS pursuant to Part III of this Exhibit.

3. To ensure that necessary corrective actions are taken, financial audit findings that are either uncontested or upheld after appeal may be used by DHCS during prospective contract negotiations.

Exhibit B, Attachment I - Funding for Fiscal Year 2017-18 through FY 2019-20

Version:	Original
Date:	7/1/2017

County:	Contract Number:
Nevada	**17-94146**

Fiscal Year 2017-18	2017-18 Funding Amount
	Original
SAPT Block Grant - FFY 2018 Award (10/1/17 to 6/30/19)	
Duns #: 010979029 Federal Grant #: 2B08TI010062-18	
CFDA: 93.959 FAIN: TI10062-18	
- Discretionary	537,420
- Prevention Set-Aside	129,638
- Friday Night Live/Club Live	6,000
- Perintal	18,124
- Adolescent/Youth	13,168
TOTAL	**704,350**

Fiscal Year 2018-19	2018-19 Funding Amount
	Original
SAPT Block Grant - FFY 2019 Award (10/1/18 to 6/30/20)	
Duns #: 010979029 Federal Grant #: 2B08TI010062-19	
CFDA: 93.959 FAIN: TI10062-19	
- Discretionary	537,420
- Prevention Set-Aside	129,638
- Friday Night Live/Club Live	6,000
- Perintal	18,124
- Adolescent/Youth	13,168
TOTAL	**704,350**

Fiscal Year 2019-20	2019-20 Funding Amount
	Original
SAPT Block Grant - FFY 2020 Award (10/1/19 to 6/30/21)	
Duns #: 010979029 Federal Grant #: 2B08TI010062-20	
CFDA: 93.959 FAIN: TI10062-20	
- Discretionary	537,420
- Prevention Set-Aside	129,638
- Friday Night Live/Club Live	6,000
- Perintal	18,124
- Adolescent/Youth	13,168
TOTAL	**704,350**

ORIGINAL THREE-YEAR TOTAL	**2,113,050**

Special Terms and Conditions

(For federally funded service contracts or agreements and grant agreements)

The use of headings or titles throughout this exhibit is for convenience only and shall not be used to interpret or to govern the meaning of any specific term or condition.

The terms "contract", "Contractor" and "Subcontractor" shall also mean, “agreement”, "grant", “grant agreement”, "Grantee" and "Subgrantee" respectively.

The terms “California Department of Health Care Services”, “California Department of Health Services”, ‘Department of Health Care Services”, “Department of Health Services”, “CDHCS”, “DHCS”, “CDHS”, and “DHS” shall all have the same meaning and refer to the California State agency that is a party to this Agreement.

This exhibit contains provisions that require strict adherence to various contracting laws and policies. Some provisions herein are conditional and only apply if specified conditions exist (i.e., agreement total exceeds a certain amount; agreement is federally funded, etc.). The provisions herein apply to this Agreement unless the provisions are removed by reference on the face of this Agreement, the provisions are superseded by an alternate provision appearing elsewhere in this Agreement, or the applicable conditions do not exist.

Index of Special Terms and Conditions

1. Federal Equal Opportunity Requirements

(Applicable to all federally funded agreements entered into by the Department of Health Care Services)

a. The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, national origin, physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. The Contractor will take affirmative action to ensure that qualified applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, national origin, physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. Such action shall include, but not be limited to the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and career development opportunities and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Federal Government or DHCS, setting forth the provisions of the Equal Opportunity clause, Section 503 of the Rehabilitation Act of 1973 and the affirmative action clause required by the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. 4212). Such notices shall state the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified applicants without discrimination based on their race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era and the rights of applicants and employees.

b. The Contractor will, in all solicitations or advancements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era.

c. The Contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding a notice, to be provided by the Federal Government or the State, advising the labor union or workers' representative of the Contractor's commitments under the provisions herein and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

d. The Contractor will comply with all provisions of and furnish all information and reports required by Section 503 of the Rehabilitation Act of 1973, as amended, the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. 4212) and of the Federal Executive Order No. 11246 as amended, including by Executive Order 11375, ‘Amending Executive Order 11246 Relating to Equal Employment Opportunity,‘ and as supplemented by regulation at 41 CFR part 60, “Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” and of the rules, regulations, and relevant orders of the Secretary of Labor.

e. The Contractor will furnish all information and reports required by Federal Executive Order No. 11246 as amended, including by Executive Order 11375, ‘Amending Executive Order 11246 Relating to Equal Employment Opportunity,‘ and as supplemented by regulation at 41 CFR part 60, “Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” and the Rehabilitation Act of 1973, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to its books, records, and accounts by the State and its designated representatives and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

f. In the event of the Contractor's noncompliance with the requirements of the provisions herein or with any federal rules, regulations, or orders which are referenced herein, this Agreement may be cancelled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further federal and state contracts in accordance with procedures authorized in Federal Executive Order No. 11246 as amended and such other sanctions may be imposed and remedies invoked as provided in Federal Executive Order No. 11246 as amended, including by Executive Order 11375, ‘Amending Executive Order 11246 Relating to Equal Employment Opportunity,‘ and as supplemented by regulation at 41 CFR part 60, “Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

g. The Contractor will include the provisions of Paragraphs a through g in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to Federal Executive Order No. 11246 as amended, including by Executive Order 11375, 'Amending Executive Order 11246 Relating to Equal Employment Opportunity,' and as supplemented by regulation at 41 CFR part 60, "Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," or Section 503 of the Rehabilitation Act of 1973 or (38 U.S.C. 4212) of the Vietnam Era Veteran's Readjustment Assistance Act, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the Director of the Office of Federal Contract Compliance Programs or DHCS may direct as a means of enforcing such provisions including sanctions for noncompliance provided, however, that in the event the Contractor becomes involved in, or is threatened with litigation by a subcontractor or vendor as a result of such direction by DHCS, the Contractor may request in writing to DHCS, who, in turn, may request the United States to enter into such litigation to protect the interests of the State and of the United States.

2. Travel and Per Diem Reimbursement

(Applicable if travel and/or per diem expenses are reimbursed with agreement funds.)

Reimbursement for travel and per diem expenses from DHCS under this Agreement shall, unless otherwise specified in this Agreement, be at the rates currently in effect, as established by the California Department of Human Resources (CalHR), for nonrepresented state employees as stipulated in DHCS' Travel Reimbursement Information Exhibit. If the CalHR rates change during the term of the Agreement, the new rates shall apply upon their effective date and no amendment to this Agreement shall be necessary. Exceptions to CalHR rates may be approved by DHCS upon the submission of a statement by the Contractor indicating that such rates are not available to the Contractor. No travel outside the State of California shall be reimbursed without prior authorization from DHCS. Verbal authorization should be confirmed in writing. Written authorization may be in a form including fax or email confirmation.

3. Procurement Rules

(Applicable to agreements in which equipment/property, commodities and/or supplies are furnished by DHCS or expenses for said items are reimbursed by DHCS with state or federal funds provided under the Agreement.)

a. **Equipment/Property definitions**

Wherever the term equipment and/or property is used, the following definitions shall apply:

(1) **Major equipment/property**: A tangible or intangible item having a base unit cost of **$5,000 or more** with a life expectancy of one (1) year or more and is either furnished by DHCS or the cost is reimbursed through this Agreement. Software and videos are examples of intangible items that meet this definition.

(2) **Minor equipment/property**: A tangible item having a base unit cost of **less than $5,000** with a life expectancy of one (1) year or more and is either furnished by DHCS or the cost is reimbursed through this Agreement.

b. **Government and public entities** (including state colleges/universities and auxiliary organizations), whether acting as a contractor and/or subcontractor, may secure all commodities, supplies, equipment and services related to such purchases that are required in performance of this Agreement. Said procurements are subject to Paragraphs d through h of Provision 3. Paragraph c of Provision 3 shall also apply, if equipment/property purchases are delegated to subcontractors that are nonprofit organizations or commercial businesses.

c. **Nonprofit organizations and commercial businesses**, whether acting as a contractor and/or subcontractor, may secure commodities, supplies, equipment/property and services related to such purchases for performance under this Agreement.

(1) Equipment/property purchases shall not exceed $50,000 annually.

To secure equipment/property above the annual maximum limit of $50,000, the Contractor shall make arrangements through the appropriate DHCS Program Contract Manager, to have all remaining

equipment/property purchased through DHCS' Purchasing Unit. The cost of equipment/property purchased by or through DHCS shall be deducted from the funds available in this Agreement. Contractor shall submit to the DHCS Program Contract Manager a list of equipment/property specifications for those items that the State must procure. DHCS may pay the vendor directly for such arranged equipment/property purchases and title to the equipment/property will remain with DHCS. The equipment/property will be delivered to the Contractor's address, as stated on the face of the Agreement, unless the Contractor notifies the DHCS Program Contract Manager, in writing, of an alternate delivery address.

(2) All equipment/property purchases are subject to Paragraphs d through h of Provision 3. Paragraph b of Provision 3 shall also apply, if equipment/property purchases are delegated to subcontractors that are either a government or public entity.

(3) Nonprofit organizations and commercial businesses shall use a procurement system that meets the following standards:

(a) Maintain a code or standard of conduct that shall govern the performance of its officers, employees, or agents engaged in awarding procurement contracts. No employee, officer, or agent shall participate in the selection, award, or administration of a procurement, or bid contract in which, to his or her knowledge, he or she has a financial interest.

(b) Procurements shall be conducted in a manner that provides, to the maximum extent practical, open, and free competition.

(c) Procurements shall be conducted in a manner that provides for all of the following:

[1] Avoid purchasing unnecessary or duplicate items.

[2] Equipment/property solicitations shall be based upon a clear and accurate description of the technical requirements of the goods to be procured.

[3] Take positive steps to utilize small and veteran owned businesses.

d. Unless waived or otherwise stipulated in writing by DHCS, prior written authorization from the appropriate DHCS Program Contract Manager will be required before the Contractor will be reimbursed for any purchase of $5,000 or more for commodities, supplies, equipment/property, and services related to such purchases. The Contractor must provide in its request for authorization all particulars necessary, as specified by DHCS, for evaluating the necessity or desirability of incurring such costs. The term "purchase" excludes the purchase of services from a subcontractor and public utility services at rates established for uniform applicability to the general public.

e. In special circumstances, determined by DHCS (e.g., when DHCS has a need to monitor certain purchases, etc.), DHCS may require prior written authorization and/or the submission of paid vendor receipts for any purchase, regardless of dollar amount. DHCS reserves the right to either deny claims for reimbursement or to request repayment for any Contractor and/or subcontractor purchase that DHCS determines to be unnecessary in carrying out performance under this Agreement.

f. The Contractor and/or subcontractor must maintain a copy or narrative description of the procurement system, guidelines, rules, or regulations that will be used to make purchases under this Agreement. The State reserves the right to request a copy of these documents and to inspect the purchasing practices of the Contractor and/or subcontractor at any time.

g. For all purchases, the Contractor and/or subcontractor must maintain copies of all paid vendor invoices, documents, bids and other information used in vendor selection, for inspection or audit. Justifications supporting the absence of bidding (i.e., sole source purchases) shall also be maintained on file by the Contractor and/or subcontractor for inspection or audit.

h. DHCS may, with cause (e.g., with reasonable suspicion of unnecessary purchases or use of inappropriate purchase practices, etc.), withhold, cancel, modify, or retract the delegated purchase authority granted under Paragraphs b and/or c of Provision 3 by giving the Contractor no less than 30 calendar days written notice.

4. Equipment/Property Ownership / Inventory / Disposition

(Applicable to agreements in which equipment/property is furnished by DHCS and/or when said items are purchased or reimbursed by DHCS with state or federal funds provided under the Agreement.)

a. Wherever the term equipment and/or property is used in Provision 4, the definitions in Paragraph a of Provision 3 shall apply.

   Unless otherwise stipulated in this Agreement, all equipment and/or property that is purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement shall be considered state equipment and the property of DHCS.

   (1) **Reporting of Equipment/Property Receipt -** DHCS requires the reporting, tagging and annual inventorying of all equipment and/or property that is furnished by DHCS or purchased/reimbursed with funds provided through this Agreement.

   Upon receipt of equipment and/or property, the Contractor shall report the receipt to the DHCS Program Contract Manager. To report the receipt of said items and to receive property tags, Contractor shall use a form or format designated by DHCS' Asset Management Unit. If the appropriate form (i.e., Contractor Equipment Purchased with DHCS Funds) does not accompany this Agreement, Contractor shall request a copy from the DHCS Program Contract Manager.

   (2) **Annual Equipment/Property Inventory -** If the Contractor enters into an agreement with a term of more than twelve months, the Contractor shall submit an annual inventory of state equipment and/or property to the DHCS Program Contract Manager using a form or format designated by DHCS' Asset Management Unit. If an inventory report form (i.e., Inventory/Disposition of DHCS-Funded Equipment) does not accompany this Agreement, Contractor shall request a copy from the DHCS Program Contract Manager. Contractor shall:

   (a) Include in the inventory report, equipment and/or property in the Contractor's possession and/or in the possession of a subcontractor (including independent consultants).

   (b) Submit the inventory report to DHCS according to the instructions appearing on the inventory form or issued by the DHCS Program Contract Manager.

   (c) Contact the DHCS Program Contract Manager to learn how to remove, trade-in, sell, transfer or survey off, from the inventory report, expired equipment and/or property that is no longer wanted, usable or has passed its life expectancy. Instructions will be supplied by either the DHCS Program Contract Manager or DHCS' Asset Management Unit.

b. Title to state equipment and/or property shall not be affected by its incorporation or attachment to any property not owned by the State.

c. Unless otherwise stipulated, DHCS shall be under no obligation to pay the cost of restoration, or rehabilitation of the Contractor's and/or Subcontractor's facility which may be affected by the removal of any state equipment and/or property.

d. The Contractor and/or Subcontractor shall maintain and administer a sound business program for ensuring the proper use, maintenance, repair, protection, insurance and preservation of state equipment and/or property.

   (1) In administering this provision, DHCS may require the Contractor and/or Subcontractor to repair or replace, to DHCS' satisfaction, any damaged, lost or stolen state equipment and/or property. In the event of state equipment and/or miscellaneous property theft, Contractor and/or Subcontractor shall immediately file a theft report with the appropriate police agency or the California Highway Patrol and Contractor shall promptly submit one copy of the theft report to the DHCS Program Contract Manager.

e. Unless otherwise stipulated by the Program funding this Agreement, equipment and/or property purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, shall only be used for performance of this Agreement or another DHCS agreement.

f. Within sixty (60) calendar days prior to the termination or end of this Agreement, the Contractor shall

provide a final inventory report of equipment and/or property to the DHCS Program Contract Manager and shall, at that time, query DHCS as to the requirements, including the manner and method, of returning state equipment and/or property to DHCS. Final disposition of equipment and/or property shall be at DHCS expense and according to DHCS instructions. Equipment and/or property disposition instructions shall be issued by DHCS immediately after receipt of the final inventory report. At the termination or conclusion of this Agreement, DHCS may at its discretion, authorize the continued use of state equipment and/or property for performance of work under a different DHCS agreement.

g. **Motor Vehicles**

(Applicable only if motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under this Agreement.)

(1) If motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, within thirty (30) calendar days prior to the termination or end of this Agreement, the Contractor and/or Subcontractor shall return such vehicles to DHCS and shall deliver all necessary documents of title or registration to enable the proper transfer of a marketable title to DHCS.

(2) If motor vehicles are purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, the State of California shall be the legal owner of said motor vehicles and the Contractor shall be the registered owner. The Contractor and/or a subcontractor may only use said vehicles for performance and under the terms of this Agreement.

(3) The Contractor and/or Subcontractor agree that all operators of motor vehicles, purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, shall hold a valid State of California driver's license. In the event that ten or more passengers are to be transported in any one vehicle, the operator shall also hold a State of California Class B driver's license.

(4) If any motor vehicle is purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, the Contractor and/or Subcontractor, as applicable, shall provide, maintain, and certify that, at a minimum, the following type and amount of automobile liability insurance is in effect during the term of this Agreement or any extension period during which any vehicle remains in the Contractor's and/or Subcontractor's possession:

Automobile Liability Insurance

(a) The Contractor, by signing this Agreement, hereby certifies that it possesses or will obtain automobile liability insurance in the amount of $1,000,000 per occurrence for bodily injury and property damage combined. Said insurance must be obtained and made effective upon the delivery date of any motor vehicle, purchased/reimbursed with agreement funds or furnished by DHCS under the terms of this Agreement, to the Contractor and/or Subcontractor.

(b) The Contractor and/or Subcontractor shall, as soon as practical, furnish a copy of the certificate of insurance to the DHCS Program Contract Manager. The certificate of insurance shall identify the DHCS contract or agreement number for which the insurance applies.

(c) The Contractor and/or Subcontractor agree that bodily injury and property damage liability insurance, as required herein, shall remain in effect at all times during the term of this Agreement or until such time as the motor vehicle is returned to DHCS.

(d) The Contractor and/or Subcontractor agree to provide, at least thirty (30) days prior to the expiration date of said insurance coverage, a copy of a new certificate of insurance evidencing continued coverage, as indicated herein, for not less than the remainder of the term of this Agreement, the term of any extension or continuation thereof, or for a period of not less than one (1) year.

(e) The Contractor and/or Subcontractor, if not a self-insured government and/or public entity, must provide evidence, that any required certificates of insurance contain the following provisions:

[1] The insurer will not cancel the insured's coverage without giving thirty (30) calendar days prior written notice to the State (California Department of Health Care Services).

[2] The State of California, its officers, agents, employees, and servants are included as additional insureds, but only with respect to work performed for the State under this Agreement and any extension or continuation of this Agreement.

[3] The insurance carrier shall notify the California Department of Health Care Services (DHCS), in writing, of the Contractor's failure to pay premiums; its cancellation of such policies; or any other substantial change, including, but not limited to, the status, coverage, or scope of the required insurance. Such notices shall contain a reference to each agreement number for which the insurance was obtained.

(f) The Contractor and/or Subcontractor is hereby advised that copies of certificates of insurance may be subject to review and approval by the Department of General Services (DGS), Office of Risk and Insurance Management. The Contractor shall be notified by DHCS, in writing, if this provision is applicable to this Agreement. If DGS approval of the certificate of insurance is required, the Contractor agrees that no work or services shall be performed prior to obtaining said approval.

(g) In the event the Contractor and/or Subcontractor fails to keep insurance coverage, as required herein, in effect at all times during vehicle possession, DHCS may, in addition to any other remedies it may have, terminate this Agreement upon the occurrence of such event.

5. Subcontract Requirements

(Applicable to agreements under which services are to be performed by subcontractors including independent consultants.)

a. Prior written authorization will be required before the Contractor enters into or is reimbursed for any subcontract for services costing $5,000 or more. Except as indicated in Paragraph a(3) herein, when securing subcontracts for services exceeding $5,000, the Contractor shall obtain at least three bids or justify a sole source award.

(1) The Contractor must provide in its request for authorization, all information necessary for evaluating the necessity or desirability of incurring such cost.

(2) DHCS may identify the information needed to fulfill this requirement.

(3) Subcontracts performed by the following entities or for the service types listed below are exempt from the bidding and sole source justification requirements:

(a) A local governmental entity or the federal government,

(b) A State college or State university from any State,

(c) A Joint Powers Authority,

(d) An auxiliary organization of a California State University or a California community college,

(e) A foundation organized to support the Board of Governors of the California Community Colleges,

(f) An auxiliary organization of the Student Aid Commission established under Education Code § 69522,

(g) Firms or individuals proposed for use and approved by DHCS' funding Program via acceptance of an application or proposal for funding or pre/post contract award negotiations,

(h) Entities and/or service types identified as exempt from advertising and competitive bidding in State Contracting Manual Chapter 5 Section 5.80 Subsection B.2. View this publication at the following Internet address: http://www.dgs.ca.gov/ols/Resources/StateContractManual.aspx.

b. DHCS reserves the right to approve or disapprove the selection of subcontractors and with advance written notice, require the substitution of subcontractors and require the Contractor to terminate subcontracts entered into in support of this Agreement.

(1) Upon receipt of a written notice from DHCS requiring the substitution and/or termination of a subcontract, the Contractor shall take steps to ensure the completion of any work in progress and

select a replacement, if applicable, within 30 calendar days, unless a longer period is agreed to by DHCS.

c. Actual subcontracts (i.e., written agreement between the Contractor and a subcontractor) of $5,000 or more are subject to the prior review and written approval of DHCS. DHCS may, at its discretion, elect to waive this right. All such waivers shall be confirmed in writing by DHCS.

d. Contractor shall maintain a copy of each subcontract entered into in support of this Agreement and shall, upon request by DHCS, make copies available for approval, inspection, or audit.

e. DHCS assumes no responsibility for the payment of subcontractors used in the performance of this Agreement. Contractor accepts sole responsibility for the payment of subcontractors used in the performance of this Agreement.

f. The Contractor is responsible for all performance requirements under this Agreement even though performance may be carried out through a subcontract.

g. The Contractor shall ensure that all subcontracts for services include provision(s) requiring compliance with applicable terms and conditions specified in this Agreement.

h. The Contractor agrees to include the following clause, relevant to record retention, in all subcontracts for services:

"(*Subcontractor Name*) agrees to maintain and preserve, until three years after termination of (*Agreement Number*) and final payment from DHCS to the Contractor, to permit DHCS or any duly authorized representative, to have access to, examine or audit any pertinent books, documents, papers and records related to this subcontract and to allow interviews of any employees who might reasonably have information related to such records."

i. Unless otherwise stipulated in writing by DHCS, the Contractor shall be the subcontractor's sole point of contact for all matters related to performance and payment under this Agreement.

j. Contractor shall, as applicable, advise all subcontractors of their obligations pursuant to the following numbered provisions of this Exhibit: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 19, 20, 24, 32 and/or other numbered provisions herein that are deemed applicable.

6. Income Restrictions

Unless otherwise stipulated in this Agreement, the Contractor agrees that any refunds, rebates, credits, or other amounts (including any interest thereon) accruing to or received by the Contractor under this Agreement shall be paid by the Contractor to DHCS, to the extent that they are properly allocable to costs for which the Contractor has been reimbursed by DHCS under this Agreement.

7. Audit and Record Retention

(Applicable to agreements in excess of $10,000.)

a. The Contractor and/or Subcontractor shall maintain books, records, documents, and other evidence, accounting procedures and practices, sufficient to properly reflect all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. The foregoing constitutes "records" for the purpose of this provision.

b. The Contractor's and/or subcontractor's facility or office or such part thereof as may be engaged in the performance of this Agreement and his/her records shall be subject at all reasonable times to inspection, audit, and reproduction.

c. Contractor agrees that DHCS, the Department of General Services, the Bureau of State Audits, or their designated representatives including the Comptroller General of the United States shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such

records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (GC 8546.7, CCR Title 2, Section 1896).

d. The Contractor and/or Subcontractor shall preserve and make available his/her records (1) for a period of three years from the date of final payment under this Agreement, and (2) for such longer period, if any, as is required by applicable statute, by any other provision of this Agreement, or by subparagraphs (1) or (2) below.

(1) If this Agreement is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of three years from the date of any resulting final settlement.

(2) If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the three-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular three-year period, whichever is later.

e. The Contractor and/or Subcontractor shall comply with the above requirements and be aware of the penalties for violations of fraud and for obstruction of investigation as set forth in Public Contract Code § 10115.10, if applicable.

f. The Contractor and/or Subcontractor may, at its discretion, following receipt of final payment under this Agreement, reduce its accounts, books and records related to this Agreement to microfilm, computer disk, CD ROM, DVD, or other data storage medium. Upon request by an authorized representative to inspect, audit or obtain copies of said records, the Contractor and/or Subcontractor must supply or make available applicable devices, hardware, and/or software necessary to view, copy and/or print said records. Applicable devices may include, but are not limited to, microfilm readers and microfilm printers, etc.

g. The Contractor shall, if applicable, comply with the Single Audit Act and the audit reporting requirements set forth in OMB Circular A-133.

8. Site Inspection

The State, through any authorized representatives, has the right at all reasonable times to inspect or otherwise evaluate the work performed or being performed hereunder including subcontract supported activities and the premises in which it is being performed. If any inspection or evaluation is made of the premises of the Contractor or Subcontractor, the Contractor shall provide and shall require Subcontractors to provide all reasonable facilities and assistance for the safety and convenience of the authorized representatives in the performance of their duties. All inspections and evaluations shall be performed in such a manner as will not unduly delay the work.

9. Federal Contract Funds

(Applicable only to that portion of an agreement funded in part or whole with federal funds.)

a. It is mutually understood between the parties that this Agreement may have been written before ascertaining the availability of congressional appropriation of funds, for the mutual benefit of both parties, in order to avoid program and fiscal delays which 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 the State by the United States Government for the fiscal years covered by the term of this Agreement. In addition, this Agreement is subject to any additional restrictions, limitations, or conditions enacted by the Congress or any statute enacted by the Congress which may affect the provisions, terms or funding of this Agreement in any manner.

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

d. DHCS has the option to invalidate or cancel the Agreement with 30-days advance written notice or to amend the Agreement to reflect any reduction in funds.

10. Intellectual Property Rights

a. Ownership

(1) Except where DHCS has agreed in a signed writing to accept a license, DHCS shall be and remain, without additional compensation, the sole owner of any and all rights, title and interest in all Intellectual Property, from the moment of creation, whether or not jointly conceived, that are made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement.

(2) For the purposes of this Agreement, Intellectual Property means recognized protectable rights and interest such as: patents, (whether or not issued) copyrights, trademarks, service marks, applications for any of the foregoing, inventions, trade secrets, trade dress, logos, insignia, color combinations, slogans, moral rights, right of publicity, author's rights, contract and licensing rights, works, mask works, industrial design rights, rights of priority, know how, design flows, methodologies, devices, business processes, developments, innovations, good will and all other legal rights protecting intangible proprietary information as may exist now and/or here after come into existence, and all renewals and extensions, regardless of whether those rights arise under the laws of the United States, or any other state, country or jurisdiction.

(a) For the purposes of the definition of Intellectual Property, "works" means all literary works, writings and printed matter including the medium by which they are recorded or reproduced, photographs, art work, pictorial and graphic representations and works of a similar nature, film, motion pictures, digital images, animation cells, and other audiovisual works including positives and negatives thereof, sound recordings, tapes, educational materials, interactive videos and any other materials or products created, produced, conceptualized and fixed in a tangible medium of expression. It includes preliminary and final products and any materials and information developed for the purposes of producing those final products. Works does not include articles submitted to peer review or reference journals or independent research projects.

(3) In the performance of this Agreement, Contractor will exercise and utilize certain of its Intellectual Property in existence prior to the effective date of this Agreement. In addition, under this Agreement, Contractor may access and utilize certain of DHCS' Intellectual Property in existence prior to the effective date of this Agreement. Except as otherwise set forth herein, Contractor shall not use any of DHCS' Intellectual Property now existing or hereafter existing for any purposes without the prior written permission of DHCS. **Except as otherwise set forth herein, neither the Contractor nor DHCS shall give any ownership interest in or rights to its Intellectual Property to the other Party.** If during the term of this Agreement, Contractor accesses any third-party Intellectual Property that is licensed to DHCS, Contractor agrees to abide by all license and confidentiality restrictions applicable to DHCS in the third-party's license agreement.

(4) Contractor agrees to cooperate with DHCS in establishing or maintaining DHCS' exclusive rights in the Intellectual Property, and in assuring DHCS' sole rights against third parties with respect to the Intellectual Property. If the Contractor enters into any agreements or subcontracts with other parties in order to perform this Agreement, Contractor shall require the terms of the Agreement(s) to include all Intellectual Property provisions. Such terms must include, but are not limited to, the subcontractor assigning and agreeing to assign to DHCS all rights, title and interest in Intellectual Property made, conceived, derived from, or reduced to practice by the subcontractor, Contractor or DHCS and which result directly or indirectly from this Agreement or any subcontract.

(5) Contractor further agrees to assist and cooperate with DHCS in all reasonable respects, and execute all documents and, subject to reasonable availability, give testimony and take all further acts reasonably necessary to acquire, transfer, maintain, and enforce DHCS' Intellectual Property rights and interests.

b. Retained Rights / License Rights

(1) Except for Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement, Contractor shall retain title to all of its Intellectual Property to the extent such Intellectual Property is in existence prior to the effective

date of this Agreement. Contractor hereby grants to DHCS, without additional compensation, a permanent, non-exclusive, royalty free, paid-up, worldwide, irrevocable, perpetual, non-terminable license to use, reproduce, manufacture, sell, offer to sell, import, export, modify, publicly and privately display/perform, distribute, and dispose Contractor's Intellectual Property with the right to sublicense through multiple layers, for any purpose whatsoever, to the extent it is incorporated in the Intellectual Property resulting from this Agreement, unless Contractor assigns all rights, title and interest in the Intellectual Property as set forth herein.

(2) Nothing in this provision shall restrict, limit, or otherwise prevent Contractor from using any ideas, concepts, know-how, methodology or techniques related to its performance under this Agreement, provided that Contractor's use does not infringe the patent, copyright, trademark rights, license or other Intellectual Property rights of DHCS or third party, or result in a breach or default of any provisions of this Exhibit or result in a breach of any provisions of law relating to confidentiality.

c. Copyright

(1) Contractor agrees that for purposes of copyright law, all works [as defined in Paragraph a, subparagraph (2)(a) of this provision] of authorship made by or on behalf of Contractor in connection with Contractor's performance of this Agreement shall be deemed "works made for hire". Contractor further agrees that the work of each person utilized by Contractor in connection with the performance of this Agreement will be a "work made for hire," whether that person is an employee of Contractor or that person has entered into an agreement with Contractor to perform the work. Contractor shall enter into a written agreement with any such person that: (i) all work performed for Contractor shall be deemed a "work made for hire" under the Copyright Act and (ii) that person shall assign all right, title, and interest to DHCS to any work product made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement.

(2) All materials, including, but not limited to, visual works or text, reproduced or distributed pursuant to this Agreement that include Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement, shall include DHCS' notice of copyright, which shall read in 3mm or larger typeface: "© *[Enter Current Year e.g., 2010, etc.]*, California Department of Health Care Services. This material may not be reproduced or disseminated without prior written permission from the California Department of Health Care Services." This notice should be placed prominently on the materials and set apart from other matter on the page where it appears. Audio productions shall contain a similar audio notice of copyright.

d. Patent Rights

With respect to inventions made by Contractor in the performance of this Agreement, which did not result from research and development specifically included in the Agreement's scope of work, Contractor hereby grants to DHCS a license as described under Section b of this provision for devices or material incorporating, or made through the use of such inventions. If such inventions result from research and development work specifically included within the Agreement's scope of work, then Contractor agrees to assign to DHCS, without additional compensation, all its right, title and interest in and to such inventions and to assist DHCS in securing United States and foreign patents with respect thereto.

e. Third-Party Intellectual Property

Except as provided herein, Contractor agrees that its performance of this Agreement shall not be dependent upon or include any Intellectual Property of Contractor or third party without first: (i) obtaining DHCS' prior written approval; and (ii) granting to or obtaining for DHCS, without additional compensation, a license, as described in Section b of this provision, for any of Contractor's or third-party's Intellectual Property in existence prior to the effective date of this Agreement. If such a license upon the these terms is unattainable, and DHCS determines that the Intellectual Property should be included in or is required for Contractor's performance of this Agreement, Contractor shall obtain a license under terms acceptable to DHCS.

f. Warranties

(1) Contractor represents and warrants that:

(a) It is free to enter into and fully perform this Agreement.

(b) It has secured and will secure all rights and licenses necessary for its performance of this Agreement.

(c) Neither Contractor's performance of this Agreement, nor the exercise by either Party of the rights granted in this Agreement, nor any use, reproduction, manufacture, sale, offer to sell, import, export, modification, public and private display/performance, distribution, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement will infringe upon or violate any Intellectual Property right, non-disclosure obligation, or other proprietary right or interest of any third-party or entity now existing under the laws of, or hereafter existing or issued by, any state, the United States, or any foreign country. There is currently no actual or threatened claim by any such third party based on an alleged violation of any such right by Contractor.

(d) Neither Contractor's performance nor any part of its performance will violate the right of privacy of, or constitute a libel or slander against any person or entity.

(e) It has secured and will secure all rights and licenses necessary for Intellectual Property including, but not limited to, consents, waivers or releases from all authors of music or performances used, and talent (radio, television and motion picture talent), owners of any interest in and to real estate, sites, locations, property or props that may be used or shown.

(f) It has not granted and shall not grant to any person or entity any right that would or might derogate, encumber, or interfere with any of the rights granted to DHCS in this Agreement.

(g) It has appropriate systems and controls in place to ensure that state funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

(h) It has no knowledge of any outstanding claims, licenses or other charges, liens, or encumbrances of any kind or nature whatsoever that could affect in any way Contractor's performance of this Agreement.

(2) DHCS MAKES NO WARRANTY THAT THE INTELLECTUAL PROPERTY RESULTING FROM THIS AGREEMENT DOES NOT INFRINGE UPON ANY PATENT, TRADEMARK, COPYRIGHT OR THE LIKE, NOW EXISTING OR SUBSEQUENTLY ISSUED.

g. Intellectual Property Indemnity

(1) Contractor shall indemnify, defend and hold harmless DHCS and its licensees and assignees, and its officers, directors, employees, agents, representatives, successors, and users of its products, ("Indemnitees") from and against all claims, actions, damages, losses, liabilities (or actions or proceedings with respect to any thereof), whether or not rightful, arising from any and all actions or claims by any third party or expenses related thereto (including, but not limited to, all legal expenses, court costs, and attorney's fees incurred in investigating, preparing, serving as a witness in, or defending against, any such claim, action, or proceeding, commenced or threatened) to which any of the Indemnitees may be subject, whether or not Contractor is a party to any pending or threatened litigation, which arise out of or are related to (i) the incorrectness or breach of any of the representations, warranties, covenants or agreements of Contractor pertaining to Intellectual Property; or (ii) any Intellectual Property infringement, or any other type of actual or alleged infringement claim, arising out of DHCS' use, reproduction, manufacture, sale, offer to sell, distribution, import, export, modification, public and private performance/display, license, and disposition of the Intellectual Property made, conceived, derived from, or reduced to practice by Contractor or DHCS and which result directly or indirectly from this Agreement. This indemnity obligation shall apply irrespective of whether the infringement claim is based on a patent, trademark or copyright registration that issued after the effective date of this Agreement. DHCS reserves the right to participate in and/or control, at Contractor's expense, any such infringement action brought against DHCS.

(2) Should any Intellectual Property licensed by the Contractor to DHCS under this Agreement become the subject of an Intellectual Property infringement claim, Contractor will exercise its authority

reasonably and in good faith to preserve DHCS' right to use the licensed Intellectual Property in accordance with this Agreement at no expense to DHCS. DHCS shall have the right to monitor and appear through its own counsel (at Contractor's expense) in any such claim or action. In the defense or settlement of the claim, Contractor may obtain the right for DHCS to continue using the licensed Intellectual Property; or, replace or modify the licensed Intellectual Property so that the replaced or modified Intellectual Property becomes non-infringing provided that such replacement or modification is functionally equivalent to the original licensed Intellectual Property. If such remedies are not reasonably available, DHCS shall be entitled to a refund of all monies paid under this Agreement, without restriction or limitation of any other rights and remedies available at law or in equity.

(3) Contractor agrees that damages alone would be inadequate to compensate DHCS for breach of any term of this Intellectual Property Exhibit by Contractor. Contractor acknowledges DHCS would suffer irreparable harm in the event of such breach and agrees DHCS shall be entitled to obtain equitable relief, including without limitation an injunction, from a court of competent jurisdiction, without restriction or limitation of any other rights and remedies available at law or in equity.

h. Federal Funding

In any agreement funded in whole or in part by the federal government, DHCS may acquire and maintain the Intellectual Property rights, title, and ownership, which results directly or indirectly from the Agreement; except as provided in 37 Code of Federal Regulations part 401.14; however, the federal government shall have a non-exclusive, nontransferable, irrevocable, paid-up license throughout the world to use, duplicate, or dispose of such Intellectual Property throughout the world in any manner for governmental purposes and to have and permit others to do so.

i. Survival

The provisions set forth herein shall survive any termination or expiration of this Agreement or any project schedule.

11. Air or Water Pollution Requirements

Any federally funded agreement and/or subcontract in excess of $100,000 must comply with the following provisions unless said agreement is exempt under 40 CFR 15.5.

a. Government contractors agree to comply with all applicable standards, orders, or requirements issued under section 306 of the Clean Air Act [42 U.S.C. 1857(h)], section 508 of the Clean Water Act (33 U.S.C. 1368), Executive Order 11738, and Environmental Protection Agency regulations (40 CFR part 15).

b. Institutions of higher education, hospitals, nonprofit organizations and commercial businesses agree to comply with all applicable standards, orders, or requirements issued under the Clean Air Act (42 U.S.C. 7401 et seq.), as amended, and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended.

12. Prior Approval of Training Seminars, Workshops or Conferences

Contractor shall obtain prior DHCS approval of the location, costs, dates, agenda, instructors, instructional materials, and attendees at any reimbursable training seminar, workshop, or conference conducted pursuant to this Agreement and of any reimbursable publicity or educational materials to be made available for distribution. The Contractor shall acknowledge the support of the State whenever publicizing the work under this Agreement in any media. This provision does not apply to necessary staff meetings or training sessions held for the staff of the Contractor or Subcontractor to conduct routine business matters.

13. Confidentiality of Information

a. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure names and other identifying information concerning persons either receiving services pursuant to this Agreement or persons whose names or identifying information become available or are disclosed to the Contractor, its employees, agents, or subcontractors as a result of services performed under this Agreement, except for statistical information not identifying any such person.

b. The Contractor and its employees, agents, or subcontractors shall not use such identifying information for any purpose other than carrying out the Contractor's obligations under this Agreement.

c. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DHCS Program Contract Manager all requests for disclosure of such identifying information not emanating from the client or person.

d. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the client, any such identifying information to anyone other than DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is required by State or Federal law.

e. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.

f. As deemed applicable by DHCS, this provision may be supplemented by additional terms and conditions covering personal health information (PHI) or personal, sensitive, and/or confidential information (PSCI). Said terms and conditions will be outlined in one or more exhibits that will either be attached to this Agreement or incorporated into this Agreement by reference.

14. Documents, Publications and Written Reports

(Applicable to agreements over $5,000 under which publications, written reports and documents are developed or produced. Government Code Section 7550.)

Any document, publication or written report (excluding progress reports, financial reports and normal contractual communications) prepared as a requirement of this Agreement shall contain, in a separate section preceding the main body of the document, the number and dollar amounts of all contracts or agreements and subcontracts relating to the preparation of such document or report, if the total cost for work by nonemployees of the State exceeds $5,000.

15. Dispute Resolution Process

a. A Contractor grievance exists whenever there is a dispute arising from DHCS' action in the administration of an agreement. If there is a dispute or grievance between the Contractor and DHCS, the Contractor must seek resolution using the procedure outlined below.

(1) The Contractor should first informally discuss the problem with the DHCS Program Contract Manager. If the problem cannot be resolved informally, the Contractor shall direct its grievance together with any evidence, in writing, to the program Branch Chief. The grievance shall state the issues in dispute, the legal authority or other basis for the Contractor's position and the remedy sought. The Branch Chief shall render a decision within ten (10) working days after receipt of the written grievance from the Contractor. The Branch Chief shall respond in writing to the Contractor indicating the decision and reasons therefore. If the Contractor disagrees with the Branch Chief's decision, the Contractor may appeal to the second level.

(2) When appealing to the second level, the Contractor must prepare an appeal indicating the reasons for disagreement with Branch Chief's decision. The Contractor shall include with the appeal a copy of the Contractor's original statement of dispute along with any supporting evidence and a copy of the Branch Chief's decision. The appeal shall be addressed to the Deputy Director of the division in which the branch is organized within ten (10) working days from receipt of the Branch Chief's decision. The Deputy Director of the division in which the branch is organized or his/her designee shall meet with the Contractor to review the issues raised. A written decision signed by the Deputy Director of the division in which the branch is organized or his/her designee shall be directed to the Contractor within twenty (20) working days of receipt of the Contractor's second level appeal.

b. If the Contractor wishes to appeal the decision of the Deputy Director of the division in which the branch is organized or his/her designee, the Contractor shall follow the procedures set forth in Health and Safety Code Section 100171.

c. Unless otherwise stipulated in writing by DHCS, all dispute, grievance and/or appeal correspondence shall be directed to the DHCS Program Contract Manager.

d. There are organizational differences within DHCS' funding programs and the management levels identified in this dispute resolution provision may not apply in every contractual situation. When a grievance is received and organizational differences exist, the Contractor shall be notified in writing by the DHCS Program Contract Manager of the level, name, and/or title of the appropriate management official that is responsible for issuing a decision at a given level.

16. Financial and Compliance Audit Requirements

a. The definitions used in this provision are contained in Section 38040 of the Health and Safety Code, which by this reference is made a part hereof.

b. Direct service contract means a contract or agreement for services contained in local assistance or subvention programs or both (see Health and Safety [H&S] Code Section 38020). Direct service contracts shall not include contracts, agreements, grants, or subventions to other governmental agencies or units of government nor contracts or agreements with regional centers or area agencies on aging (H&S Code Section 38030).

c. The Contractor, as indicated below, agrees to obtain one of the following audits:

(1) ***If the Contractor is a nonprofit organization (as defined in H&S Code Section 38040)*** and receives **$25,000 or more** from any State agency under a direct service contract or agreement; the Contractor agrees to obtain an annual single, organization wide, financial and compliance audit. Said audit shall be conducted according to Generally Accepted Auditing Standards. This audit does not fulfill the audit requirements of Paragraph c(3) below. The audit shall be completed by the 15th day of the fifth month following the end of the Contractor's fiscal year, **and/or**

(2) ***If the Contractor is a nonprofit organization (as defined in H&S Code Section 38040)*** and receives **less than $25,000** per year from any State agency under a direct service contract or agreement, the Contractor agrees to obtain a biennial single, organization wide financial and compliance audit, unless there is evidence of fraud or other violation of state law in connection with this Agreement. This audit does not fulfill the audit requirements of Paragraph c(3) below. The audit shall be completed by the 15th day of the fifth month following the end of the Contractor's fiscal year, **and/or**

(3) ***If the Contractor is a State or Local Government entity or Nonprofit organization (as defined by the Federal Office of Management and Budget [OMB] Circular A-133)*** and expends $500,000 or more in Federal awards, the Contractor agrees to obtain an annual single, organization wide, financial and compliance audit according to the requirements specified in OMB Circular A-133 entitled "Audits of States, Local Governments, and Non-Profit Organizations". An audit conducted pursuant to this provision will fulfill the audit requirements outlined in Paragraphs c(1) and c(2) above. The audit shall be completed by the end of the ninth month following the end of the audit period. The requirements of this provision apply if:

(a) The Contractor is a recipient expending Federal awards received directly from Federal awarding agencies, or

(b) The Contractor is a subrecipient expending Federal awards received from a pass-through entity such as the State, County or community based organization.

(4) If the Contractor submits to DHCS a report of an audit other than an OMB A-133 audit, the Contractor must also submit a certification indicating the Contractor has not expended $500,000 or more in federal funds for the year covered by the audit report.

d. Two copies of the audit report shall be delivered to the DHCS program funding this Agreement. The audit report must identify the Contractor's legal name and the number assigned to this Agreement. The audit report shall be due within 30 days after the completion of the audit. Upon receipt of said audit report, the DHCS Program Contract Manager shall forward the audit report to DHCS' Audits and Investigations Unit

if the audit report was submitted under Section 16.c(3), unless the audit report is from a City, County, or Special District within the State of California whereby the report will be retained by the funding program.

e. The cost of the audits described herein may be included in the funding for this Agreement up to the proportionate amount this Agreement represents of the Contractor's total revenue. The DHCS program funding this Agreement must provide advance written approval of the specific amount allowed for said audit expenses.

f. The State or its authorized designee, including the Bureau of State Audits, is responsible for conducting agreement performance audits which are not financial and compliance audits. Performance audits are defined by Generally Accepted Government Auditing Standards.

g. Nothing in this Agreement limits the State's responsibility or authority to enforce State law or regulations, procedures, or reporting requirements arising thereto.

h. Nothing in this provision limits the authority of the State to make audits of this Agreement, provided however, that if independent audits arranged for by the Contractor meet Generally Accepted Governmental Auditing Standards, the State shall rely on those audits and any additional audit work and shall build upon the work already done.

i. The State may, at its option, direct its own auditors to perform either of the audits described above. The Contractor will be given advance written notification, if the State chooses to exercise its option to perform said audits.

j. The Contractor shall include a clause in any agreement the Contractor enters into with the audit firm doing the single organization wide audit to provide access by the State or Federal Government to the working papers of the independent auditor who prepares the single organization wide audit for the Contractor.

k. Federal or state auditors shall have "expanded scope auditing" authority to conduct specific program audits during the same period in which a single organization wide audit is being performed, but the audit report has not been issued. The federal or state auditors shall review and have access to the current audit work being conducted and will not apply any testing or review procedures which have not been satisfied by previous audit work that has been completed.

   The term "expanded scope auditing" is applied and defined in the U.S. General Accounting Office (GAO) issued Standards for *Audit of Government Organizations, Programs, Activities and Functions*, better known as the "yellow book".

17. Human Subjects Use Requirements

(Applicable only to federally funded agreements/grants in which performance, directly or through a subcontract/subaward, includes any tests or examination of materials derived from the human body.)

By signing this Agreement, Contractor agrees that if any performance under this Agreement or any subcontract or subagreement includes any tests or examination of materials derived from the human body for the purpose of providing information, diagnosis, prevention, treatment or assessment of disease, impairment, or health of a human being, all locations at which such examinations are performed shall meet the requirements of 42 U.S.C. Section 263a (CLIA) and the regulations thereunder.

18. Novation Requirements

If the Contractor proposes any novation agreement, DHCS shall act upon the proposal within 60 days after receipt of the written proposal. DHCS may review and consider the proposal, consult and negotiate with the Contractor, and accept or reject all or part of the proposal. Acceptance or rejection of the proposal may be made orally within the 60-day period and confirmed in writing within five days of said decision. Upon written acceptance of the proposal, DHCS will initiate an amendment to this Agreement to formally implement the approved proposal.

19. Debarment and Suspension Certification

(Applicable to all agreements funded in part or whole with federal funds.)

a. By signing this Agreement, the Contractor/Grantee agrees to comply with applicable federal suspension and debarment regulations including, but not limited to 7 CFR Part 3017, 45 CFR 76, 40 CFR 32 or 34 CFR 85.

b. By signing this Agreement, the Contractor certifies to the best of its knowledge and belief, that it and its principals:

(1) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency;

(2) Have not within a three-year period preceding this application/proposal/agreement been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(3) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in Paragraph b(2) herein; and

(4) Have not within a three-year period preceding this application/proposal/agreement had one or more public transactions (Federal, State or local) terminated for cause or default.

(5) Shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under federal regulations (i.e., 48 CFR part 9, subpart 9.4), debarred, suspended, declared ineligible, or voluntarily excluded from participation in such transaction, unless authorized by the State.

(6) Will include a clause entitled, "Debarment and Suspension Certification" that essentially sets forth the provisions herein, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

c. If the Contractor is unable to certify to any of the statements in this certification, the Contractor shall submit an explanation to the DHCS Program Contract Manager.

d. The terms and definitions herein have the meanings set out in the Definitions and Coverage sections of the rules implementing Federal Executive Order 12549.

e. If the Contractor knowingly violates this certification, in addition to other remedies available to the Federal Government, the DHCS may terminate this Agreement for cause or default.

20. Smoke-Free Workplace Certification

(Applicable to federally funded agreements/grants and subcontracts/subawards, that provide health, day care, early childhood development services, education or library services to children under 18 directly or through local governments.)

a. Public Law 103-227, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, early childhood development services, education or library services to children under the age of 18, if the services are funded by federal programs either directly or through state or local governments, by federal grant, contract, loan, or loan guarantee. The law also applies to children's services that are provided in indoor facilities that are constructed, operated, or maintained with such federal funds. The law does not apply to children's services provided in private residences; portions of facilities used for inpatient drug or alcohol treatment; service providers whose sole source of applicable federal funds is Medicare or Medicaid; or facilities where WIC coupons are redeemed.

b. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to $1,000 for each violation and/or the imposition of an administrative compliance order on the responsible party.

c. By signing this Agreement, Contractor or Grantee certifies that it will comply with the requirements of the Act and will not allow smoking within any portion of any indoor facility used for the provision of services for children as defined by the Act. The prohibitions herein are effective December 26, 1994.

d. Contractor or Grantee further agrees that it will insert this certification into any subawards (subcontracts or subgrants) entered into that provide for children's services as described in the Act.

21. Covenant Against Contingent Fees

(Applicable only to federally funded agreements.)

The Contractor warrants that no person or selling agency has been employed or retained to solicit/secure this Agreement upon an agreement of understanding for a commission, percentage, brokerage, or contingent fee, except *bona fide* employees or *bona fide* established commercial or selling agencies retained by the Contractor for the purpose of securing business. For breach or violation of this warranty, DHCS shall have the right to annul this Agreement without liability or in its discretion to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such commission, percentage, and brokerage or contingent fee.

22. Payment Withholds

(Applicable only if a final report is required by this Agreement. Not applicable to government entities.)

Unless waived or otherwise stipulated in this Agreement, DHCS may, at its discretion, withhold 10 percent (10%) of the face amount of the Agreement, 50 percent (50%) of the final invoice, or $3,000 whichever is greater, until DHCS receives a final report that meets the terms, conditions and/or scope of work requirements of this Agreement.

23. Performance Evaluation

(Not applicable to grant agreements.)

DHCS may, at its discretion, evaluate the performance of the Contractor at the conclusion of this Agreement. If performance is evaluated, the evaluation shall not be a public record and shall remain on file with DHCS. Negative performance evaluations may be considered by DHCS prior to making future contract awards.

24. Officials Not to Benefit

No members of or delegate of Congress or the State Legislature shall be admitted to any share or part of this Agreement, or to any benefit that may arise therefrom. This provision shall not be construed to extend to this Agreement if made with a corporation for its general benefits.

25. Four-Digit Date Compliance

(Applicable to agreements in which Information Technology (IT) services are provided to DHCS or if IT equipment is procured.)

Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Deliverables and/or services to the State. "Four Digit Date compliant" Deliverables and services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.

26. Prohibited Use of State Funds for Software

(Applicable to agreements in which computer software is used in performance of the work.)

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

27. Use of Small, Minority Owned and Women's Businesses

(Applicable to that portion of an agreement that is federally funded and entered into with institutions of higher education, hospitals, nonprofit organizations or commercial businesses.)

Positive efforts shall be made to use small businesses, minority-owned firms and women's business enterprises, whenever possible (i.e., procurement of goods and/or services). Contractors shall take all of the following steps to further this goal.

(1) Ensure that small businesses, minority-owned firms, and women's business enterprises are used to the fullest extent practicable.

(2) Make information on forthcoming purchasing and contracting opportunities available and arrange time frames for purchases and contracts to encourage and facilitate participation by small businesses, minority-owned firms, and women's business enterprises.

(3) Consider in the contract process whether firms competing for larger contracts intend to subcontract with small businesses, minority-owned firms, and women's business enterprises.

(4) Encourage contracting with consortiums of small businesses, minority-owned firms and women's business enterprises when a contract is too large for one of these firms to handle individually.

(5) Use the services and assistance, as appropriate, of such organizations as the Federal Small Business Administration and the U.S. Department of Commerce's Minority Business Development Agency in the solicitation and utilization of small businesses, minority-owned firms and women's business enterprises.

28. Alien Ineligibility Certification

(Applicable to sole proprietors entering federally funded agreements.)

By signing this Agreement, the Contractor certifies that he/she is not an alien that is ineligible for state and local benefits, as defined in Subtitle B of the Personal Responsibility and Work Opportunity Act. (8 U.S.C. 1601, et seq.)

29. Union Organizing

(Applicable only to grant agreements.)

Grantee, by signing this Agreement, hereby acknowledges the applicability of Government Code Sections 16645 through 16649 to this Agreement. Furthermore, Grantee, by signing this Agreement, hereby certifies that:

a. No state funds disbursed by this grant will be used to assist, promote or deter union organizing.

b. Grantee shall account for state funds disbursed for a specific expenditure by this grant, to show those funds were allocated to that expenditure.

c. Grantee shall, where state funds are not designated as described in b herein, allocate, on a pro-rata basis, all disbursements that support the grant program.

d. If Grantee makes expenditures to assist, promote or deter union organizing, Grantee will maintain records sufficient to show that no state funds were used for those expenditures, and that Grantee shall provide those records to the Attorney General upon request.

30. Contract Uniformity (Fringe Benefit Allowability)

(Applicable only to nonprofit organizations.)

Pursuant to the provisions of Article 7 (commencing with Section 100525) of Chapter 3 of Part 1 of Division 101 of the Health and Safety Code, DHCS sets forth the following policies, procedures, and guidelines regarding the reimbursement of fringe benefits.

a. As used herein fringe benefits shall mean an employment benefit given by one's employer to an employee in addition to one's regular or normal wages or salary.

b. As used herein, fringe benefits do not include:

(1) Compensation for personal services paid currently or accrued by the Contractor for services of employees rendered during the term of this Agreement, which is identified as regular or normal salaries and wages, annual leave, vacation, sick leave, holidays, jury duty and/or military leave/training.
(2) Director's and executive committee member's fees.
(3) Incentive awards and/or bonus incentive pay.
(4) Allowances for off-site pay.
(5) Location allowances.
(6) Hardship pay.
(7) Cost-of-living differentials

c. Specific allowable fringe benefits include:

(1) Fringe benefits in the form of employer contributions for the employer's portion of payroll taxes (i.e., FICA, SUI, SDI), employee health plans (i.e., health, dental and vision), unemployment insurance, worker's compensation insurance, and the employer's share of pension/retirement plans, provided they are granted in accordance with established written organization policies and meet all legal and Internal Revenue Service requirements.

d. To be an allowable fringe benefit, the cost must meet the following criteria:

(1) Be necessary and reasonable for the performance of the Agreement.
(2) Be determined in accordance with generally accepted accounting principles.
(3) Be consistent with policies that apply uniformly to all activities of the Contractor.

e. Contractor agrees that all fringe benefits shall be at actual cost.

f. Earned/Accrued Compensation

(1) Compensation for vacation, sick leave and holidays is limited to that amount earned/accrued within the agreement term. Unused vacation, sick leave and holidays earned from periods prior to the agreement term cannot be claimed as allowable costs. See Provision f (3)(a) for an example.

(2) For multiple year agreements, vacation and sick leave compensation, which is earned/accrued but not paid, due to employee(s) not taking time off may be carried over and claimed within the overall term of the multiple years of the Agreement. Holidays cannot be carried over from one agreement year to the next. See Provision f (3)(b) for an example.

(3) For single year agreements, vacation, sick leave and holiday compensation that is earned/accrued but not paid, due to employee(s) not taking time off within the term of the Agreement, cannot be claimed as an allowable cost. See Provision f (3)(c) for an example.

(a) **Example No. 1:**

If an employee, John Doe, earns/accrues three weeks of vacation and twelve days of sick leave each year, then that is the maximum amount that may be claimed during a one year agreement. If John Doe has five weeks of vacation and eighteen days of sick leave at the beginning of an agreement, the Contractor during a one-year budget period may only claim up to three weeks of vacation and twelve days of sick leave as actually used by the employee. Amounts earned/accrued in periods prior to the beginning of the Agreement are not an allowable cost.

(b) **Example No. 2:**

If during a three-year (multiple year) agreement, John Doe does not use his three weeks of vacation in year one, or his three weeks in year two, but he does actually use nine weeks in year three; the Contractor would be allowed to claim all nine weeks paid for in year three. The total compensation over the three-year period cannot exceed 156 weeks (3 x 52 weeks).

(c) **Example No. 3:**

If during a single year agreement, John Doe works fifty weeks and used one week of vacation and one week of sick leave and all fifty-two weeks have been billed to DHCS, the remaining unused two weeks of vacation and seven days of sick leave may not be claimed as an allowable cost.

31. Suspension or Stop Work Notification

a. DHCS may, at any time, issue a notice to suspend performance or stop work under this Agreement. The initial notification may be a verbal or written directive issued by the funding Program's Contract Manager. Upon receipt of said notice, the Contractor is to suspend and/or stop all, or any part, of the work called for by this Agreement.

b. Written confirmation of the suspension or stop work notification with directions as to what work (if not all) is to be suspended and how to proceed will be provided within 30 working days of the verbal notification. The suspension or stop work notification shall remain in effect until further written notice is received from DHCS. The resumption of work (in whole or part) will be at DHCS' discretion and upon receipt of written confirmation.

(1) Upon receipt of a suspension or stop work notification, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize or halt the incurrence of costs allocable to the performance covered by the notification during the period of work suspension or stoppage.

(2) Within 90 days of the issuance of a suspension or stop work notification, DHCS shall either:

(a) Cancel, extend, or modify the suspension or stop work notification; or

(b) Terminate the Agreement as provided for in the Cancellation / Termination clause of the Agreement.

c. If a suspension or stop work notification issued under this clause is canceled or the period of suspension or any extension thereof is modified or expires, the Contractor may resume work only upon written concurrence of funding Program's Contract Manager.

d. If the suspension or stop work notification is cancelled and the Agreement resumes, changes to the services, deliverables, performance dates, and/or contract terms resulting from the suspension or stop work notification shall require an amendment to the Agreement.

e. If a suspension or stop work notification is not canceled and the Agreement is cancelled or terminated pursuant to the provision entitled Cancellation / Termination, DHCS shall allow reasonable costs resulting from the suspension or stop work notification in arriving at the settlement costs.

f. DHCS shall not be liable to the Contractor for loss of profits because of any suspension or stop work notification issued under this clause.

32. Lobbying Restrictions and Disclosure Certification

(Applicable to federally funded agreements in excess of $100,000 per Section 1352 of the 31, U.S.C.)

a. Certification and Disclosure Requirements

(1) Each person (or recipient) who requests or receives a contract or agreement, subcontract, grant, or subgrant, which is subject to Section 1352 of the 31, U.S.C., and which exceeds $100,000 at any tier, shall file a certification (in the form set forth in Attachment 1, consisting of one page, entitled "Certification Regarding Lobbying") that the recipient has not made, and will not make, any payment prohibited by Paragraph b of this provision.

(2) Each recipient shall file a disclosure (in the form set forth in Attachment 2, entitled "Standard Form-LLL 'disclosure of Lobbying Activities'") if such recipient has made or has agreed to make any payment using nonappropriated funds (to include profits from any covered federal action) in connection with a contract, or grant or any extension or amendment of that contract, or grant, which would be prohibited under Paragraph b of this provision if paid for with appropriated funds.

(3) Each recipient shall file a disclosure form at the end of each calendar quarter in which there occurs any event that requires disclosure or that materially affect the accuracy of the information contained in any disclosure form previously filed by such person under Paragraph a(2) herein. An event that materially affects the accuracy of the information reported includes:

(a) A cumulative increase of $25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered federal action;

(b) A change in the person(s) or individuals(s) influencing or attempting to influence a covered federal action; or

(c) A change in the officer(s), employee(s), or member(s) contacted for the purpose of influencing or attempting to influence a covered federal action.

(4) Each person (or recipient) who requests or receives from a person referred to in Paragraph a(1) of this provision a contract or agreement, subcontract, grant or subgrant exceeding $100,000 at any tier under a contract or agreement, or grant shall file a certification, and a disclosure form, if required, to the next tier above.

(5) All disclosure forms (but not certifications) shall be forwarded from tier to tier until received by the person referred to in Paragraph a(1) of this provision. That person shall forward all disclosure forms to DHCS Program Contract Manager.

b. Prohibition

Section 1352 of Title 31, U.S.C., provides in part that no appropriated funds may be expended by the recipient of a federal contract or agreement, grant, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered federal actions: the awarding of any federal contract or agreement, the making of any federal grant, the making of any federal loan, entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract or agreement, grant, loan, or cooperative agreement.

Attachment 1
State of California
Department of Health Care Services

CERTIFICATION REGARDING LOBBYING

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making, awarding or entering into of this Federal contract, Federal grant, or cooperative agreement, and the extension, continuation, renewal, amendment, or modification of this Federal contract, grant, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency of the United States Government, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, “Disclosure of Lobbying Activities" in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontractors, subgrants, and contracts under grants and cooperative agreements) of $100,000 or more, and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S.C., any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

County of Nevada	Hank Weston
Name of Contractor	Printed Name of Person Signing for Contractor
17-94146	
Contract / Grant Number	Signature of Person Signing for Contractor
	Chair, Board of Supervisors
Date	Title

After execution by or on behalf of Contractor, please return to:

California Department of Health Care Services

DHCS reserves the right to notifiy the contractor in writing of an alternate submission address.

Attachment 2

CERTIFICATION REGARDING LOBBYING

Approved by OMB
0348-0046

Complete this form to disclose lobbying activities pursuant to 31 U.S.C. 1352
(See reverse for public burden disclosure)

1. Type of Federal Action:	2. Status of Federal Action:	3. Report Type:
[ ] a. contract b. grant c. cooperative agreement d. loan e. loan guarantee f. loan insurance	[ ] a. bid/offer/application b. initial award c. post-award	[ ] a. initial filing b. material change For Material Change Only: Year _____ quarter _____ date of last report _____.

4. Name and Address of Reporting Entity:	5. If Reporting Entity in No. 4 is Subawardee, Enter Name and Address of Prime:
☐ Prime ☐ Subawardee Tier ___, if known: Congressional District, If known:	Congressional District, If known:
6. Federal Department/Agency	7. Federal Program Name/Description: CDFA Number, if applicable: _____
8. Federal Action Number, if known:	9. Award Amount, if known: $
10.a. Name and Address of Lobbying Registrant *(If individual, last name, first name, MI)*:	b. Individuals Performing Services *(including address if different from 10a.* *(Last name, First name, MI):*
11. Information requested through this form is authorized by title 31 U.S.C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U.S.C. 1352. This information will be available for public inspection. Any person that fails to file the required disclosure shall be subject to a not more than $100,000 for each such failure.	Signature: _____ Print Name: _____ Title: Telephone No.: Date:

Federal Use Only	Authorized for Local Reproduction Standard Form-LLL (Rev. 7-97)

INSTRUCTIONS FOR COMPLETION OF SF-LLL, DISCLOSURE OF LOBBYING ACTIVITIES

This disclosure form shall be completed by the reporting entity, whether subawardee or prime Federal recipient, at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying activity is and/or has been secured to influence the outcome of a covered Federal action.

2. Identify the status of the covered Federal action.

3. Identify the appropriateclassification of this report. If this is a followup report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.

4. Enter the full name, address, city, State and zip code of the reporting entity. Include Congressional District, if known. Check the appropriate classification of the reporting entity that designates if itis, or expects to be,a prime or subaward recipient. Identify the tier of the subawardee, e.g., the first subawardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grants.

5. If the organization filing the report in item 4 checks "Subawardee," then enter the full name, address, city, State and zip code of the prime Federal recipient. Include Congressional District, if known.

6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizationallevel below agency name, if known. For example, Department of Transportation, United States Coast Guard.

7. Enter the Federal program name or description for the covered Federal action (item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans, and loan commitments.

8. Enter the most appropriate Federal identifying number available for the Federal action identified in item 1 (e.g., Request for Proposal (RFP) number; Invitation for Bid (IFB) number; grant announcement number; the contract, grant, or loan award number; the application/proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP-DE-90-001".

9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the prime entity identified in item 4 or 5.

10. (a) Enter the full name, address, city, State and zip code of the lobbying registrant under the Lobbying Disclosure Act of 1995 engaged by the reporting entity identified in item 4 to influence the covered Federal action.

    (b) Enter the full names of the individual(s) performing services, and include full address if different from 10 (a). Enter Last Name, First Name, and Middle Initial (MI).

11. The certifying official shall sign and date the form, print his/her name, title, and telephone number.

According to the Paperwork Reduction Act, as amended, no persons are required to respond to a collection of information unless it displays a valid OMB Control Number. The valid OMB control number for this information collection is OMB No. 0348-0046. Public reporting burden for this collection of information is estimated to average 10 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0046), Washington, DC 20503.

Exhibit E
Additional Provisions

1. Amendment Process

A. The Department of Health Care Services (DHCS) may amend the Contract.

B. Should either party, during the term of this Agreement, desire a change or amendment to the terms of this Agreement, such changes or amendments shall be proposed in writing to the other party, who will respond in writing as to whether the proposed changes/amendments are accepted or rejected. If accepted and after negotiations are concluded, the agreed upon changes shall be made through the State's official agreement amendment process. No amendment will be considered binding on either party until it is formally approved by the both parties and the Department of General Services (DGS), if DGS approval is required.

C. Contract amendments will be required to change encumbered amounts for each year of a multi-year contract period, of which the first amendment will be based on the Governor's Budget Act allocation of that specific fiscal year. The signed contract from the Contractor will be due to DHCS within 90 days from the issuance to the County. If the signed Contract from the Contractor is not received within 90 days from the issuance to the County, DHCS may withhold all non-DMC payments under Exhibit B of this Contract until the required amendment is received by the State.

D. Contract amendments may be requested by the Contractor until May 1 of each of the contract's fiscal years. An amendment proposed by either the Contractor or the State shall be forwarded in writing to the other party.

1) The proposed amendment submitted by Contractor shall include the proposed changes, and a statement of the reason and basis for the proposed change.

2) Amendments shall be duly approved by the County Board of Supervisors or its authorized designee, and signed by a duly authorized representative.

E. Contractor acknowledges that any newly allocated funds that are in excess of the initial amount for each fiscal year may be forfeited if DHCS does not receive a fully executable contract amendment on or before June 30, 2018.

F. State may settle costs for substance use disorder services based on the year-end cost settlement report as the final amendment to the approved single State/County contract.

2. Cancellation / Termination

A. This Agreement may be cancelled by DHCS without cause upon 30 calendar days advance written notice to the Contractor.

Exhibit E

B. DHCS reserves the right to cancel or terminate this Agreement immediately for cause. The Contractor may submit a written request to terminate this Agreement only if DHCS substantially fails to perform its responsibilities as provided herein.

C. The term "for cause" shall mean that the Contractor fails to meet the terms, conditions, and/or responsibilities of this Agreement.

D. Agreement termination or cancellation shall be effective as of the date indicated in DHCS' notification to the Contractor. The notice shall stipulate any final performance, invoicing or payment requirements.

E. Upon receipt of a notice of termination or cancellation, the Contractor shall take immediate steps to stop performance and to cancel or reduce subsequent agreement costs.

F. In the event of early termination or cancellation, the Contractor shall be entitled to payment for all allowable costs authorized under this Agreement and incurred up to the date of termination or cancellation, including authorized non-cancelable obligations, provided such expenses do not exceed the stated maximum amounts payable.

G. In the event of changes in law that affect provisions of this Contract, the parties agree to amend the affected provisions to conform to the changes in law retroactive to the effective date of such changes in law. The parties further agree that the terms of this Contract are severable and in the event that changes in law render provisions of the Contract void, the unaffected provisions and obligations of this Contract will remain in full force and effect.

H. In the event this Contract is terminated, Contractor shall deliver its entire fiscal and program records pertaining to the performance of this Contract to DHCS, which will retain the records for the required retention period.

3. Avoidance of Conflicts of Interest by Contractor

A. DHCS intends to avoid any real or apparent conflict of interest on the part of the Contractor, subcontractors, or employees, officers and directors of the Contractor or subcontractors. Thus, DHCS reserves the right to determine, at its sole discretion, whether any information, assertion or claim received from any source indicates the existence of a real or apparent conflict of interest; and, if a conflict is found to exist, to require the Contractor to submit additional information or a plan for resolving the conflict, subject to DHCS review and prior approval.

B. Conflicts of interest include, but are not limited to:

1) An instance where the Contractor or any of its subcontractors, or any employee, officer, or director of the Contractor or any subcontractor has an interest, financial or otherwise, whereby the use or disclosure of information obtained while performing services under the Agreement would allow for private or personal benefit or for any purpose that is contrary to the goals and objectives of the Agreement.

2) An instance where the Contractor's or any subcontractor's employees, officers, or directors use their positions for purposes that are, or give the appearance of being, motivated by a desire for private gain for themselves or others, such as those with whom they have family, business or other ties.

C. If DHCS is or becomes aware of a known or suspected conflict of interest, the Contractor will be given an opportunity to submit additional information or to resolve the conflict. A Contractor with a suspected conflict of interest will have five (5) working days from the date of notification of the conflict by DHCS to provide complete information regarding the suspected conflict. If a conflict of interest is determined to exist by DHCS and cannot be resolved to the satisfaction of DHCS, the conflict will be grounds for terminating the Agreement. DHCS may, at its discretion upon receipt of a written request from the Contractor, authorize an extension of the timeline indicated herein.

D. Contractor acknowledges that state laws on conflict of interest, found in the Political Reform Act, Public Contract Code Section 10365.5, and Government Code Section 1090, apply to this Contract.

4. Freeze Exemptions

(Applicable only to local government agencies.)

A. Contractor agrees that any hiring freeze adopted during the term of this Agreement shall not be applied to the positions funded, in whole or part, by this Agreement.

B. Contractor agrees not to implement any personnel policy, which may adversely affect performance or the positions funded, in whole or part, by this Agreement.

C. Contractor agrees that any travel freeze or travel limitation policy adopted during the term of this Agreement shall not restrict travel funded, in whole or part, by this Agreement.

D. Contractor agrees that any purchasing freeze or purchase limitation policy adopted during the term of this Agreement shall not restrict or limit purchases funded, in whole or part, by this Agreement.

5. Domestic Partners

Pursuant to Public Contract Code 10295.3, no state agency may enter into any contract executed or amended after January 1, 2007, for the acquisition of goods or services in the amount of $100,000 or more with a contractor who, in the provision of benefits, discriminates between employees with spouses and employees with domestic partners, or discriminates between domestic partners and spouses of those employees.

6. Force Majeure

Neither party shall be responsible for delays or failures in performance resulting from acts beyond the control of the offending party. Such acts shall include but not be limited to acts of God, fire, flood, earthquake, other natural disaster, nuclear accident, strike, lockout, riot, freight-embargo, related-utility, or governmental statutes or regulations super-imposed after the fact. If a delay or failure in performance by the Contractor arises out of a default of its Subcontractor, and if such default of its Subcontractor, arises out of causes beyond the control of both the Contractor and Subcontractor, and without the fault or negligence of either of them, the Contractor shall not be liable for damages of such delay or failure, unless the supplies or services to be furnished by the Subcontractor were obtainable from other sources in sufficient time to permit the Contractor to meet the required performance schedule.

Exhibit F
Privacy and Information Security Provisions

This Exhibit F is intended to protect the privacy and security of specified Department information that the Contractor may access, receive, or transmit under this Agreement. The Department information covered under this Exhibit F consists of: (1) Protected Health Information as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA")(PHI) and (2) Personal Information (PI) as defined under the California Information Practices Act (CIPA), at California Civil Code Section 1798.3. Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit F consists of the following parts:

1. Exhibit F-1, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.

2. Exhibit F-2, which provides for the privacy and security of PI in accordance with specified provisions of the Agreement between the Department and the Social Security Administration, known as the Information Exchange Agreement (IEA) and the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (Computer Agreement) to the extent Contractor access, receives, or transmits PI under these Agreements. Exhibit F-2 further provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.

3. Exhibit F-3, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit F in its entirety.

Exhibit F
Privacy and Information Security Provisions

F1
HIPAA Business Associate Addendum

1. Recitals.

A. A business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. Section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") and the Final Omnibus Rule of 2013 between Department and Contractor arises only to the extent that Contractor creates, receives, maintains, transmits, uses or discloses PHI or ePHI on the Department's behalf, or provides services, arranges, performs, or assists in the performance of functions or activities on behalf of the Department that are included in the definition of "business associate" in 45 CFR. 160.103 where the provision of the service involves the disclosure of PHI or ePHI from the Department, including but not limited to, utilization review, quality assurance, or benefit management. To the extent Contractor performs these services, functions, and activities on behalf of Department, Contractor is the Business Associate of the Department, acting on the Department's behalf. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties." A business associate is also directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or sub-award to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.

B. The Department wishes to disclose to Contractor certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under Federal law, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit F-1 of this Agreement. This information is hereafter referred to as "Department PHI".

C. The purpose of this Exhibit F-1 is to protect the privacy and security of the PHI and ePHI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations and the Final Omnibus Rule of 2013, including, but not limited to, the requirement that the Department must enter into a contract containing specific requirements

with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act and the Final Omnibus Rule of 2013. To the extent that data is both PHI or ePHI and Personally Identifying Information, both Exhibit F-2 (including Attachment I, the SSA Agreement between SSA, CHHS and DHCS, referred to in Exhibit F-2) and this Exhibit F-1 shall apply.

D. The terms used in this Exhibit F-1, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

2. Definitions.

A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations and the Final Omnibus Rule of 2013.

B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations and the Final Omnibus Rule of 2013.

C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, HIPAA regulations and the Final Omnibus of 2013.

D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit F-1 of this Agreement. The terms PHI as used in this document shall mean Department PHI.

E. Electronic Health Records shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921 and implementing regulations.

F. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

G. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to

believe the information can be used to identify the individual, as set forth under 45 CFR Section 160.103.

H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 CFR Parts 160 and 164, subparts A and E.

I. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR Section 160.103 and as defined under HIPAA.

J. Required by law, as set forth under 45 CFR Section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit F-1 of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.

M. Security Rule shall mean the HIPAA regulations that are found at 45 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. Section 17932(h), any guidance issued by the Secretary pursuant to such Act and the HIPAA regulations.

3. Terms of Agreement.

A. **Permitted Uses and Disclosures of Department PHI by Contractor.**

Except as otherwise indicated in this Exhibit F-1, Contractor may use or disclose Department PHI only to perform functions, activities, or services specified in Section 1.A of Exhibit F-1 of this Agreement, for, or on behalf of the Department,

provided that such use or disclosure would not violate the HIPAA regulations or the limitations set forth in 42 CFR Part 2, or any other applicable law, if done by the Department. Any such use or disclosure, if not for purposes of treatment activities of a health care provider as defined by the Privacy Rule, must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR Section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

B. **Specific Use and Disclosure Provisions**. Except as otherwise indicated in this Exhibit F-1, Contractor may:

1) **Use and Disclose for Management and Administration**. Use and disclose Department PHI for the proper management and administration of the Contractor's business, provided that such disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed, in accordance with section D(7) of this Exhibit F-1, that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware that the confidentiality of the information has been breached.

2) **Provision of Data Aggregation Services**. Use Department PHI to provide data aggregation services to the Department to the extent requested by the Department and agreed to by Contractor. Data aggregation means the combining of PHI created or received by the Contractor, as the Business Associate, on behalf of the Department with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the Department

C. **Prohibited Uses and Disclosures**

1) Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. Section 17935(a) and 45 CFR Section 164.522(a).

2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI.

Exhibit F
Privacy and Information Security Provisions

D. **Responsibilities of Contractor**

Contractor agrees:

1) **Nondisclosure**. Not to use or disclose Department PHI other than as permitted or required by this Agreement or as required by law, including but not limited to 42 CFR Part 2.

2) **Compliance with the HIPAA Security Rule**. To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 CFR Sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR Section 164, subpart C, in compliance with 45 CFR Section 164.316. 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 the Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.

3) **Security**. Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

   a. Complying with all of the data system security precautions listed in Attachment A, Data Security Requirements.

   b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement.

   c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.

4) **Security Officer**. Contractor shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with

the Department.

5) **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit F.

6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit F of which it becomes aware.

7) **Contractor's Agents and Subcontractors**.

a. To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor with respect to such Department PHI under this Exhibit F, and that require compliance with all applicable provisions of HIPAA, the HITECH Act the HIPAA regulations, and the Final Omnibus Rule of 2013 including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI. As required by HIPAA, the HITECH Act, the HIPAA regulations and the Final Omnibus Rule of 2013 , including 45 CFR Sections 164.308 and 164.314, Contractor shall incorporate, when applicable, the relevant provisions of this Exhibit F-1 into each subcontract or sub-award to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI be reported to Contractor.

b. In accordance with 45 CFR Section 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:

i) Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by the Department; or

ii) Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

Exhibit F
Privacy and Information Security Provisions

8) **Availability of Information to the Department and Individuals to Provide Access and Information:**

a. To provide access as the Department may require, and in the time and manner designated by the Department (upon reasonable notice and during Contractor's normal business hours) to Department PHI in a Designated Record Set, to the Department (or, as directed by the Department), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained for the Department health plan under this Agreement that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for the Department health plan for which Contractor is providing services under this Agreement; or those records used to make decisions about individuals on behalf of the Department. Contractor shall use the forms and processes developed by the Department for this purpose and shall respond to requests for access to records transmitted by the Department within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

b. If Contractor maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. Section 17935(e) and the HIPAA regulations.

9) **Confidentiality of Alcohol and Drug Abuse Patient Records.** Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

10) **Amendment of Department PHI**. To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 CFR Section 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty days within which to make the amendment.

11) **Internal Practices**. To make Contractor's internal practices, books, and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's compliance with the HIPAA regulations. If any information

needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.

12) **Documentation of Disclosures**. To document and make available to the Department or (at the direction of the Department) to an individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR Section 164.528 and 42 U.S.C. Section 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009 and later, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

13) **Breaches and Security Incidents.** During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

a. **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call or email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours (one hour if SSA data) by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit F-1 or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Information Protection Unit (916) 445-4646, (866) 866-0602 or by emailing privacyofficer@dhcs.ca.gov. Notice shall be made using the DHCS “Privacy Incident Report” form, including all information known at the time. Contractor shall use the most

current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI, Contractor shall take:

i) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment.

ii) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

b. **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Information Protection Unit.

c. **Complete Report**. To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised

or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

d. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary (after obtaining prior written approval of DHCS). If a breach of unsecured Department PHI involves more than 500 residents of the State of California or under its jurisdiction, Contractor shall first notify DHCS, then the Secretary of the breach immediately upon discovery of the breach. If a breach involves more than 500 California residents, Contractor shall also provide, after obtaining written prior approval of DHCS, notice to the Attorney General for the State of California, Privacy Enforcement Section. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents, or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

e. **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or Federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days after discovery of the breach. The Department Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

f. **Department Contact Information**. To direct communications to the above referenced Department staff, the Contractor shall

Exhibit F
Privacy and Information Security Provisions

initiate contact as indicated herein. The Department reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Department Program Contract Manager	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Exhibit A, Scope of Work for Program Contract Manager information	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646; (866) 866-0602 Email: privacyofficer@dhcs.ca.gov Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000; (800) 579-0874 Fax: (916) 440-5537

14) **Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Contractor knows of a material breach or violation by the Department of this Exhibit F-1, it shall take the following steps:

a. Provide an opportunity for the Department to cure the breach or end the violation and terminate the Agreement if the Department does not cure the breach or end the violation within the time specified by Contractor or

b. Immediately terminate the Agreement if the Department has breached a material term of the Exhibit F-1 and cure is not possible.

15) **Sanctions and/or Penalties**. Contractor understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Contractors may result in the imposition of sanctions and/or penalties on Contractor under HIPAA, the HITECH Act and the HIPAA regulations.

Exhibit F
Privacy and Information Security Provisions

E. Obligations of the Department.

The Department agrees to:

1) **Permission by Individuals for Use and Disclosure of PHI**. Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

2) **Notification of Restrictions**. Notify the Contractor of any restriction to the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.

3) **Requests Conflicting with HIPAA Rules**. Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.

4) **Notice of Privacy Practices**. Provide Contractor with the web link to the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Visit the DHCS website to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/NoticeofPrivacyPractices.aspx or the DHCS website at www.dhcs.ca.gov (select "Privacy in the right column and "Notice of Privacy Practices" on the right side of the page).

F. Audits, Inspection and Enforcement

If Contractor is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office for Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Exhibit F-1,Contractor shall immediately notify the Department. Upon request from the Department, Contractor shall provide the Department with a copy of any Department PHI that Contractor, as the Business Associate, provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI to the Secretary. Contractor is responsible for any civil penalties assessed due to an audit or investigation of Contractor, in accordance with 42 U.S.C. Section 17934(c).

G. Termination.

1) **Term.** The Term of this Exhibit F-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(J).

2) **Termination for Cause**. In accordance with 45 CFR Section 164.504(e)(1)(iii), upon the Department's knowledge of a material breach or

Exhibit F
Privacy and Information Security Provisions

violation of this Exhibit F-1 by Contractor, the Department shall:

a. Provide an opportunity for Contractor to cure the breach or end the violation and terminate this Agreement if Contractor does not cure the breach or end the violation within the time specified by the Department or

b. Immediately terminate this Agreement if Contractor has breached a material term of this Exhibit F-1 and cure is not possible.

F-2
Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA

1. Recitals.

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:

1) The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.).

2) The Agreement between the Social Security Administration (SSA) and the Department, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA is attached to this Exhibit F as Attachment I and is hereby incorporated in this Agreement.

3) Title 42 CFR, Chapter I, Subchapter A, Part 2.

B. The purpose of this Exhibit F-2 is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for, or on behalf of Department, pursuant to this Agreement. Specifically this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in Exhibit F-1 of this Agreement, the HIPAA Business Associate Addendum; however, to the extent that data is both PHI or ePHI and PII, both Exhibit F-1 and this Exhibit F-2 shall apply.

C. The IEA Agreement referenced in A. 2) above requires the Department to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from DHCS that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities,

and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides DHCS data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

D. The terms used in this Exhibit F-2, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions.

A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).

C. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).

D. "Department PI" shall mean Personal Information, as defined below, accessed in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the Department.

E. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).

F. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

G. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

Exhibit F
Privacy and Information Security Provisions

H. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code Section 1798.3(a).

I. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

J. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

A. **Permitted Uses and Disclosures of Department PI and PII by Contractor**

Except as otherwise indicated in this Exhibit F-2, Contractor may use or disclose Department PI only to perform functions, activities or services for or on behalf of the Department pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the Department.

B. **Responsibilities of Contractor**

Contractor agrees:

1) Nondisclosure. Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and Federal law.

2) Safeguards. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which

incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;

b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III-Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment I and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.

4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit F-2.

5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit F-2 on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.

6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection,

amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.

7) Cooperation with DHCS. With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of errors in Department PI, production of Department PI, disclosure of a security breach involving Department PI and notice of such breach to the affected individual(s).

8) Confidentiality of Alcohol and Drug Abuse Patient Records. Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

9) Breaches and Security Incidents. During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

a. Initial Notice to the Department. (1) To notify the Department **immediately by telephone call or email or fax** upon the discovery of a breach of unsecured Department PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving Department PII. (2) To notify the Department **within one (1) hour by email or fax** if the data is data subject to the SSA Agreement; and **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII in violation of this Agreement or this Exhibit F-1 or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

b. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic Department PI or PII, notice shall be provided by calling the Department

Exhibit F
Privacy and Information Security Provisions

Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx .

c. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII, Contractor shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

d. **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Information Security Officer.

e. **Complete Report**. To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the

completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

f. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, section 1798.29and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

g. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

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

Exhibit F
Privacy and Information Security Provisions

Department Program Contract Manager	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Exhibit A, Scope of Work for Program Contract Manager information	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646 Email: privacyofficer@dhcs.ca.gov Telephone:(916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874 Fax: (916) 440-5537

10) Designation of Individual Responsible for Security

Contractor shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Exhibit F-2 and for communicating on security matters with the Department.

Exhibit F
Privacy and Information Security Provisions

F-3
Miscellaneous Terms and Conditions

Applicable to Exhibit F

1) **Confidentiality of Alcohol and Drug Abuse Patient Records.** Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

2) **Disclaimer**. The Department makes no warranty or representation that compliance by Contractor with this Exhibit F, HIPAA or the HIPAA regulations will be adequate or satisfactory for Contractor's own purposes or that any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of the Department PHI, PI and PII.

3) **Amendment**. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit F may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and Federal laws. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit F embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and Federal laws. The Department may terminate this Agreement upon thirty (30) days written notice in the event:

a) Contractor does not promptly enter into negotiations to amend this Exhibit F when requested by the Department pursuant to this section; or

b) Contractor does not enter into an amendment providing assurances regarding the safeguarding of Department PHI that the Department deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

4) **Judicial or Administrative Proceedings**. Contractor will notify the Department if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The Department may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The Department may terminate this Agreement if a finding or stipulation that the Contractor has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Contractor is a party or has been joined. DHCS will

consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

5) **Assistance in Litigation or Administrative Proceedings**. Contractor shall make itself and any subcontractors, employees, or agents assisting Contractor in the performance of its obligations under this Agreement, available to the Department at no cost to the Department to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Department, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

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

7) **Interpretation**. The terms and conditions in this Exhibit F shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree that any ambiguity in the terms and conditions of this Exhibit F shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and Federal laws.

8) **Conflict.** In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

9) **Regulatory References**. A reference in the terms and conditions of this Exhibit F to a section in the HIPAA regulations means the section as in effect or as amended.

10) **Survival.** The respective rights and obligations of Contractor under Section 3, Item D of Exhibit F-1, and Section 3, Item B of Exhibit F-2, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.

11) **No Waiver of Obligations**. No change, waiver, or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

Exhibit F
Privacy and Information Security Provisions

12) Audits, Inspection and Enforcement. From time to time, and subject to all applicable Federal and state privacy and security laws and regulations, the Department may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit F. Contractor shall promptly remedy any violation of any provision of this Exhibit F. The fact that the Department inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit F. The Department's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the Department's enforcement rights under this Agreement, including this Exhibit F.

13) Due Diligence. Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit F and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and Federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit F.

14) Term. The Term of this Exhibit F-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(I), and when all Department PI and PII is destroyed in accordance with Attachment A.

14) Effect of Termination. Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all Department PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the Department of the conditions that make the return or destruction infeasible, and the Department and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit F to such Department PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to Department PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

Exhibit F
Privacy and Information Security Provisions

Attachment I
Business Associate Data Security Requirements

I. Personnel Controls

A. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

B. ***Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. ***Confidentiality Statement.*** All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, 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 DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

D. ***Background Check.*** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

A. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

B. ***Server Security.*** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. ***Minimum Necessary.*** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

Exhibit F
Privacy and Information Security Provisions

D. ***Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical 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 maximum, all applicable patches must be installed within 30 days of vendor release.

G. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

H. ***Data Destruction.*** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

I. ***System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. ***Warning Banners.*** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. ***System Logging*****.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. 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. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. ***Access Controls.*** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

M. ***Transmission encryption.*** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

N. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

A. ***System Security Review.*** All systems processing and/or storing DHCS PHI or PI 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 should include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI 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 backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

Exhibit F
Privacy and Information Security Provisions

V. Paper Document Controls

A. ***Supervision of Data.*** DHCS PHI or PI 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. DHCS PHI or PI 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 DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. ***Removal of Data.*** DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

E. ***Faxing.*** Faxes containing DHCS PHI or PI 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 the fax.

F. ***Mailing.*** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

A. PURPOSE: The purpose of this Information Exchange Agreement ("IEA") is to establish terms, conditions, and safeguards under which SSA will disclose to the State Agency certain information, records, or data (herein "data") to assist the State Agency in administering certain federally funded, state-administered benefit programs (including state-funded, state supplementary payment programs under Title XVI of the Social Security Act) identified in this IEA. By entering into this IEA, the State Agency agrees to comply with:

- the terms and conditions set forth in the Computer Matching and Privacy Protection Act Agreement ("CMPPA Agreement") attached as **Attachment 1**, governing the State Agency's use of the data disclosed from SSA's Privacy Act System of Records; and
- all other terms and conditions set forth in this IEA and Attachments 2 through 6.

B. PROGRAMS AND DATA EXCHANGE SYSTEMS: (1) The State Agency will use the data received or accessed from SSA under this IEA for the purpose of administering the federally funded, state-administered programs identified in **Table 1** below. In **Table 1**, the State Agency has identified: (a) each federally funded, state-administered program that it administers; and (b) each SSA data exchange system to which the State Agency needs access in order to administer the identified program. The list of SSA's data exchange systems is attached as **Attachment 2**. **Attachment 2** provides a brief explanation of each system, as well as use parameters, as necessary.

TABLE 1

FEDERALLY FUNDED BENEFIT PROGRAMS	
Program	**SSA Data Exchange System(s)**
☒ Medicaid	BENDEX/SDX/SVES IV/SOLQ/SVES-1-Citizenship/Quarters of Coverage/PUPS
☐ Temporary Assistance to Needy Families (TANF)	
☐ Supplemental Nutrition Assistance Program (SNAP- formally Food Stamps)	
☐ Unemployment Compensation	
☐ State Child Support Agency	
☐ Low-Income Home Energy Assistance Program (LI-HEAP)	
☐ Workers Compensation	
☐ Vocational Rehabilitation Services	

☐ Foster Care (IV-E)	
☒ State Children's Health Insurance Program (CHIP)	BENDEX/SDX/SVES IV,SVES-1 Citizenship
☐ Women, Infants and Children (W.I.C.)	
☒ Medicare Savings Programs (MSP)	LIS File
☒ Medicare 1144 (Outreach)	Medicare 1144 Outreach File
☒ *Other Federally Funded, State-Administered Programs (List Below)*	
Program	**SSA Data Exchange System(s)**
Medi-Cal Access Program (MCAP)	BENDEX/SDX/SVES IV

(2) The State Agency will use each identified data exchange system ***only*** for the purpose of administering the specific program for which access to the data exchange system is provided. SSA data exchange systems are protected by the Privacy Act and Federal law prohibits the use of SSA's data for any purpose other than the purpose of administering the specific program for which such data is disclosed. In particular, the State Agency will:

a) use the **tax return data** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a program listed in 26 U.S.C. § 6103(1)(7) and (8).

b) use **citizenship status data** disclosed by SSA only to determine entitlement of *new applicants* to: (a) the Medicaid program and CHIP pursuant to the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA to receive the *SSA Data Set* through the Centers for Medicare & Medicaid Services' (CMS) Federal Data Services Hub (Hub).

Applicants for Social Security numbers (SSN) report their citizenship data at the time they apply for their SSNs; there is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

C. PROGRAM QUESTIONNAIRE: Prior to signing this IEA, the State Agency will complete and submit to SSA a program questionnaire for each of the federally funded, state-administered programs checked in **Table 1** above. SSA will not disclose any data under this IEA until it has received and approved the completed program questionnaire for each of the programs identified in **Table 1** above.

D. TRANSFER OF DATA: SSA will transmit the data to the State Agency under this IEA using the data transmission method identified in **Table 2** below:

TABLE 2

TRANSFER OF DATA
☐ Data will be transmitted directly between SSA and the State Agency.
☒ Data will be transmitted directly between SSA and The California Office of Technology (State Transmission/Transfer Component ("STC")) by File Transfer Management System (FTMS), a secure mechanism approved by SSA. The STC will serve as the conduit between SSA and the State Agency pursuant to the State STC Agreement.
☐ Data will be transmitted directly between SSA and CMS' Hub by a secure method of transfer approved by SSA. CMS will transmit the *SSA Data Set* between SSA and the State Agency pursuant to an agreement between SSA and CMS regarding the use of the Hub.
☐ Data will be transmitted [*select one:* directly between SSA and the Interstate Connection Network ("ICON") *or* through the [name of STC Agency/Vendor] as the conduit between SSA and the Interstate Connection Network ("ICON")]. ICON is a wide area telecommunications network connecting state agencies that administer the state unemployment insurance laws. When receiving data through ICON, the State Agency will comply with the "Systems Security Requirements for SSA Web Access to SSA Information Through the ICON," attached as **Attachment 3**.

E. SECURITY PROCEDURES: The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," attached as **Attachment 4**, as well as the Security Certification Requirements for use of the *SSA Data Set* transmitted via CMS' Hub, attached as **Attachment 5**. The SSA security controls identified under **Attachment 4** of this IEA prevail for all SSA data received by the State Agency, as identified in Table 1 of this IEA. For any tax return data, the State Agency will also comply with the "Tax Information Security Guidelines for Federal, State and Local Agencies," Publication 1075, published by the Secretary of the Treasury and available at the following Internal Revenue Service (IRS) website: http://www.irs.gov/pub/irs-pdf/p1075.pdf. This IRS Publication 1075 is incorporated by reference into this IEA.

F. STATE AGENCY'S RESPONSIBILITIES: The State Agency will not direct individuals to SSA field offices to obtain data that the State Agency is authorized to receive under this IEA in accordance with Table 1. Where disparities exist between individual-supplied data and SSA's data, the State Agency will take the following steps before referring the individual to an SSA field office:

- Check its records to be sure that the data of the original submission has not changed (e.g., last name recently changed);
- Contact the individual to verify the data submitted is accurate; and,
- Consult with the SSA Regional Office Contact to discuss options before advising individuals to contact SSA for resolution. The Regional Office Contact will inform the State Agency of the current protocol through which the individual should contact SSA, i.e., visiting the field office, calling the national network service number, or creating an online account via *my* Social Security.

G. CONTRACTOR/AGENT RESPONSIBILITIES: The State Agency will restrict access to the data obtained from SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this IEA. At SSA's request, the State Agency will obtain from each of its contractors and agents a current list of the employees of its contractors and agents who have access to SSA data disclosed under this IEA. The State Agency will require its contractors, agents, and all employees of such contractors or agents with authorized access to the SSA data disclosed under this IEA, to comply with the terms and conditions set forth in this IEA, and not to duplicate, disseminate, or disclose such data without obtaining SSA's prior written approval. In addition, the State Agency will comply with the limitations on use, duplication, and redisclosure of SSA data set forth in Section IX. of the CMPPA Agreement, especially with respect to its contractors and agents.

H. SAFEGUARDING AND REPORTING RESPONSIBILITIES FOR PERSONALLY IDENTIFIABLE INFORMATION ("PII"):

1. The State Agency will ensure that its employees, contractors, and agents:
   a. properly safeguard PII furnished by SSA under this IEA from loss, theft, or inadvertent disclosure;
   b. understand that they are responsible for safeguarding this information at all times, regardless of whether or not the State employee, contractor, or agent is at his or her regular duty station;
   c. ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected;
   d. send emails containing PII only if encrypted or if to and from addresses that are secure; and
   e. limit disclosure of the information and details relating to a PII loss only to those with a need to know.

2. If an employee of the State Agency or an employee of the State Agency's contractor or agent becomes aware of suspected or actual loss of PII, he or she must immediately contact the State Agency official responsible for Systems Security designated below or his or her delegate. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified below. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center at 1-877-697-4889. The responsible State Agency official or delegate will use the worksheet, attached as **Attachment 6**, to quickly gather and

organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

3. SSA will make the necessary contact within SSA to file a formal report in accordance with SSA procedures. SSA will notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to a data exchange under this IEA occurs.

4. If the State Agency experiences a loss or breach of data, it will determine whether or not to provide notice to individuals whose data has been lost or breached and bear any costs associated with the notice or any mitigation.

I. POINTS OF CONTACT:

FOR SSA

San Francisco Regional Office:
Nancy Borjon
Data Exchange Coordinator
Frank Hagel Federal Building
1221 Nevin Avenue
Richmond, CA 94801
Phone: (510) 970-8256
Fax: (510) 970-8101
Email: Nancy.Borjon@ssa.gov

Data Exchange Issues:
Sarah Reagan
Government Information Specialist
Office of the General Counsel
Office of Privacy and Disclosure
617 Altmeyer
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-9127
Fax: (410) 594-0115
Email: Sarah.Reagan@ssa.gov

Program and Policy Issues:
Michael Wilkins
State Liaison Program Manager
Office of Retirement and Disability Policy
Office of Data Exchange and Policy Publications
Office of Data Exchange
3609 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 966-4965
Fax: (410) 966-4054
Email: Michael.Wilkins@ssa.gov

Systems Security Issues:
Sean Hagan, Acting Director
Division of Compliance and Assessments
Office of Information Security
Office of Systems
Social Security Administration
3829 Annex Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-4519
Fax: (410) 597-0845
Email: Sean.Hagan@ssa.gov

Systems Issues:
Michelle J. Anderson, Branch Chief
DBIAE/Data Exchange and Verification Branch

Office of Information Technology Business Support
Office of Systems
3-D-1 Robert M. Ball Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: (410) 965-5943
Fax: (410) 966-3147
Email: Michelle.J.Anderson@ssa.gov

FOR STATE AGENCY

Agreement Issues:

Rocky Evans
Chief, Eligibility Administration Section
Program Review Branch
Medi-Cal Eligibility Division (MCED)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 319-8434
Fax: (916) 552-9477
Email: Rocky.Evans@dhcs.ca.gov

Technical Issues:

YK Chalamcherla
Chief, Application Development & Support Branch
Enterrprise Innovative Technology Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 322-8044
Fax: (916) 440-7065
Email: YK.Chalamcherla@dhcs.ca.gov

Sean Wieland
Chief, Business & Application Integration Section
Enterprise Innovative Technology Services (EITS)
1501 Capitol Avenue
Sacramento, CA 95814
Phone: (916) 550-7088
Fax: (916) 440-7065
Email: Sean.Wieland@dhcs.ca.gov

J. **DURATION:** The effective date of this IEA is March 6, 2017. This IEA will remain in effect for as long as: (1) a CMPPA Agreement governing this IEA is in effect between SSA and the State or the State Agency; and (2) the State Agency submits a certification in accordance with Section K. below at least 30 days before the expiration and renewal of such CMPPA Agreement.

K. **CERTIFICATION AND PROGRAM CHANGES:** At least 30 days before the expiration and renewal of the State CMPPA Agreement governing this IEA, the State Agency will certify in writing to SSA that: (1) it is in compliance with the terms and conditions of this IEA; (2) the data exchange processes under this IEA have been and will be conducted without change; and (3) it will, upon SSA's request, provide audit reports or other documents that demonstrate review and oversight activities. If there are substantive changes in any of the programs or data exchange processes listed in this IEA, the parties will modify the IEA in

accordance with Section L. below and the State Agency will submit for SSA's approval new program questionnaires under Section C. above describing such changes prior to using SSA's data to administer such new or changed program.

L. MODIFICATION: Modifications to this IEA must be in writing and agreed to by the parties.

M. TERMINATION: The parties may terminate this IEA at any time upon mutual written consent. In addition, either party may unilaterally terminate this IEA upon 90 days advance written notice to the other party. Such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this IEA, or terminate this IEA, if SSA, in its sole discretion, determines that the State Agency (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of SSA-supplied data; or (2) violated or failed to follow the terms and conditions of this IEA or the CMPPA Agreement.

N. INTEGRATION: This IEA, including all attachments, constitutes the entire agreement of the parties with respect to its subject matter. There have been no representations, warranties, or promises made outside of this IEA. This IEA shall take precedence over any other document that may be in conflict with it.

ATTACHMENTS

1 – CMPPA Agreement
2 – SSA Data Exchange Systems
3 – Systems Security Requirements for SSA Web Access to SSA Information Through ICON
4 – Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration
5 – Security Certification Requirements for use of the *SSA Data Set* Transmitted via CMS' Hub
6 – PII Loss Reporting Worksheet

O. AUTHORIZED SIGNATURES: The signatories below warrant and represent that they have competent authority on behalf of their respective agency to enter into the obligations set forth in this IEA.

SOCIAL SECURITY ADMINISTRATION
REGION IX

Grace M. Kim
Regional Commissioner
05/03/2017
Date

THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

Jennifer Kent
Director, California Department of Health Care Services
4/7/17
Date

CERTIFICATION OF COMPLIANCE
FOR
THE INFORMATION EXCHANGE AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION (SSA)
AND
THE CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES (STATE AGENCY)

(State Agency Level)

In accordance with the terms of the Information Exchange Agreement (IEA/F) between SSA and the State Agency, the State Agency, through its authorized representative, hereby certifies that, as of the date of this certification:

1. The State Agency is in compliance with the terms and conditions of the IEA/F;

2. The State Agency has conducted the data exchange processes under the IEA/F without change, except as modified in accordance with the IEA/F;

3. The State Agency will continue to conduct the data exchange processes under the IEA/F without change, except as may be modified in accordance with the IEA/F;

4. Upon SSA's request, the State Agency will provide audit reports or other documents that demonstrate compliance with the review and oversight activities required under the IEA/F and the governing Computer Matching and Privacy Protection Act Agreement; and

5. In compliance with the requirements of the "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration," (last updated July 2015) Attachment 4 to the IEA/F, as periodically updated by SSA, the State Agency has not made any changes in the following areas that could potentially affect the security of SSA data:

    - General System Security Design and Operating Environment
    - System Access Control
    - Automated Audit Trail
    - Monitoring and Anomaly Detection
    - Management Oversight
    - Data and Communications Security
    - Contractors of Electronic Information Exchange Partners
    - Cloud Service Providers for Electronic Information Exchange Partners

The State Agency will submit an updated Security Design Plan at least 30 days prior to making any changes to the areas listed above and provide updated contractor employee lists before allowing new employees' access to SSA provided data.

6. The State Agency agrees that use of computer technology to transfer the data is more economical, efficient, and faster than using a manual process. As such, the State Agency will continue to utilize data exchange to obtain data it needs to administer the programs for which it is authorized, under the IEA/F. Further, before directing an individual to an SSA field office to obtain data, the State Agency will verify that the information it submitted to SSA via data exchange is correct, and verify with the individual that the information he/she supplied is accurate. The use of electronic data exchange expedites program administration and limits SSA field office traffic.

The signatory below warrants and represents that he or she is a representative of the State Agency duly authorized to make this certification on behalf of the State Agency.

DEPARTMENT OF HEALTH CARE SERVICES OF CALIFORNIA

Jennifer Kent
Director

5/17/17
Date

ATTACHMENT 1

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT

(CMPPA)

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT BETWEEN THE SOCIAL SECURITY ADMINISTRATION AND THE HEALTH AND HUMAN SERVICES AGENCY OF CALIFORNIA

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement (Agreement) between the Social Security Administration (SSA) and the Health and Human Services Agency of California (State Agency) sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein as "data") made by SSA to the State Agency that administers federally funded benefit programs, including those under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-funded state supplementary payment programs under Title XVI of the Act. The terms and conditions of this Agreement ensure that SSA makes such disclosures of data, and the State Agency uses such disclosed data, in accordance with the requirements of the Privacy Act of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State Agency is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State Agency in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State Agency's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 453, 1106(b), and 1137 of the Act (42 U.S.C. §§ 653, 1306(b), and 1320b-7) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 402(x)(3)(B)(iv)) and Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii)) (prisoner data);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA), Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State Agency must follow with regard to use, treatment, and safeguarding of data.

II. Scope

A. The State Agency will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA.

B. The State Agency will execute an Information Exchange Agreement (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by the State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.

C. The State Agency will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for one or more of the following programs, which are specifically identified in the IEA:

1. Temporary Assistance to Needy Families (TANF) program under Part A of Title IV of the Act;
2. Medicaid provided under an approved State plan or an approved waiver under Title XIX of the Act;
3. State Children's Health Insurance Program (CHIP) under Title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;

4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under Titles I, X, XIV, or XVI of the Act;
11. Foster Care and Adoption Assistance under Title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by the State Agency under Titles I, IV, X, XIV, XVI, XVIII, XIX, XX, and XXI of the Act; and
14. Any other federally funded programs administered by the State Agency that are compatible with SSA's programs.

D. The State Agency will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with the State Agency are necessary for SSA to assist the State Agency in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

The State Agency will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State Agency's program criteria. A cost-benefit analysis for the exchange made under this Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records (SOR)

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications;
- 60-0059 -- Earnings Recording and Self-Employment Income System;
- 60-0090 -- Master Beneficiary Record;
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB);
- 60-0269 -- Prisoner Update Processing System (PUPS); and
- 60-0321 -- Medicare Part D and Part D Subsidy File.

The State Agency will only use the tax return data contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information. Specific listings of data elements are available at:

http://www.ssa.gov/dataexchange/

C. Number of Records Involved

The maximum number of records involved in this matching activity is the number of records maintained in SSA's SORs listed above in Section IV.A.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

The State Agency will notify all individuals who apply for federally funded, state-administered benefits that any data they provide are subject to verification through computer matching with SSA. The State Agency and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

The State Agency will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

The State Agency will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;

2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and

3. Clearly state that, unless the individual responds to the notice in the required time period, the State Agency will conclude that the SSA data are correct and will effectuate the planned action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

Pursuant to 5 U.S.C. § 552a(p)(1)(A)(ii), SSA's DIB has determined that the State Agency may use SSA's benefit data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when the benefit record is created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, the State Agency must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

Based on SSA's Office of Quality Review "Fiscal Year 2014 Enumeration Accuracy Report," the SSA Enumeration System database (the Master Files of SSN Holders and SSN Applications System) used for SSN matching is 99 percent accurate for records updated by SSA employees.

Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. The State Agency must independently verify citizenship data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

VII. Disposition and Records Retention of Matched Items

A. The State Agency will retain all data received from SSA to administer programs governed by this Agreement only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

B. The State Agency may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing the State Agency's retention of records.

C. The State Agency may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing the State Agency's retention of records.

D. The State Agency may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.

E. SSA will delete electronic data input files received from the State Agency after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

SSA and the State Agency will comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, available at http://www.irs.gov. In addition, SSA

and the State Agency will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency, including SSA's *Electronic Information Exchange Security Requirements and Procedures for State and local Agencies Exchanging Electronic Information with SSA*, as well as specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

SSA has the right to monitor the State Agency's compliance with FISMA, the terms of this Agreement, and the IEA and to make onsite inspections of the State Agency for purposes of auditing compliance, if necessary, during the lifetime of this Agreement or of any extension of this Agreement. This right includes onsite inspection of any entity that receives SSA information from the State Agency under the terms of this Agreement, if SSA determines it is necessary.

IX. Records Usage, Duplication, and Redisclosure Restrictions

A. The State Agency will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.

B. The State Agency will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. The State Agency will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.

2. The State Agency will not extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement. In limited circumstances that are approved by SSA, the State Agency may extract information about an individual other than the applicant/recipient when the applicant/recipient has provided identifying information about the individual and the individual's income or resources affect the applicant's/recipient's eligibility for such program.

3. The State Agency will not disclose to an applicant/recipient information about another individual (i.e., an applicant's household member) without the written consent from the individual to whom the information pertains.

4. The State Agency will use the Federal tax information (FTI) disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement

programs in accordance with 26 U.S.C. § 6103(l)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision IRS Publication 1075.

5. The State Agency will use the citizenship status data disclosed by SSA only to determine entitlement of new applicants to: (a) the Medicaid program and CHIP pursuant to CHIPRA, Pub. L. 111-3; or (b) federally funded, state-administered health or income maintenance programs approved by SSA. The State Agency will further comply with additional terms and conditions regarding use of citizenship data, as set forth in the State Agency's IEA.

6. The State Agency will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.

7. The State Agency will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. The State Agency will provide its contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, the State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

8. If the State Agency is authorized or required – pursuant to an applicable law, regulation, or intra-governmental documentation – to provide SSA data to another State or local government entity for the administration of the federally funded, state-administered programs covered by this Agreement, the State Agency must ensure that the State or local government entity, including its employees, abides by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement and the IEA. At SSA's request, the State Agency will provide copies of any applicable law, regulation, or intra-governmental documentation that authorizes the intra-governmental relationship with the State or local government entity. Upon request from SSA, the State Agency will also establish how it ensures that State or local government entity complies with the terms of this Agreement and the IEA.

9. The State Agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement

may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

10. The State Agency will conduct triennial compliance reviews of its contractor(s) and agent(s) no later than three years after the initial approval of the security certification to SSA. The State Agency will share documentation of its recurring compliance reviews with its contractor(s) and agent(s) with SSA. The State Agency will provide documentation to SSA during its scheduled compliance and certification reviews or upon request.

C. The State Agency will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. The State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use. To the extent SSA approves the requested redisclosure, the State Agency will ensure that any entity receiving the redisclosed data will comply with the procedures and limitations on use, duplication, and redisclosure of SSA data, as well as all administrative, technical, and physical security requirements governing all data SSA provides electronically to the State Agency including specific guidance on safeguarding and reporting responsibilities for PII, as set forth in this Agreement and the accompanying IEAs.

X. Comptroller General Access

The Comptroller General (the Government Accountability Office) may have access to all records of the State Agency that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(l)(K).

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from July 1, 2017 (Effective Date) through December 31, 2018 (Expiration Date).

2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the

Effective Date; and (c) send the required report to OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:

   - the applicable data exchange will continue without any change; and
   - SSA and the State Agency certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.

4. If either SSA or the State Agency does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State Agency has violated or failed to comply with this Agreement.

XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State Agency the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to the State Agency under any IEAs governed by this Agreement. Furthermore, SSA

is not liable for any damages or loss resulting from the destruction of any materials or data provided by the State Agency.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

XIV. Points of Contact

A. SSA Point of Contact

San Francisco Regional Office:
Jamie Lucero, Director
San Francisco Regional Office, Center for Disability and Programs Support
1221 Nevin Ave., 6th Floor
Richmond, CA 94801
Phone: 510-970-8297
Fax: 510-970-8101
Email: Jamie.Lucero@ssa.gov

B. State Agency Point of Contact

Sonia Herrera
California Health and Human Services Agency
1600 Ninth Street
Sacramento, CA 95814
Phone: 916-654-3459 / Fax: 916-440-5001
Email: Sonia.Herrera@chhs.ca.gov

XV. SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION

Mary Ann Zimmerman

Mary Ann Zimmerman
Acting Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

December 21, 2016
Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Glenn Sklar
Acting Chair
SSA Data Integrity Board

1/30/17
Date

XVI. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agency to enter into the obligations set forth in this Agreement.

SOCIAL SECURITY ADMINISTRATION

Grace M. Kim
Regional Commissioner
San Francisco

6/2/17
Date

HEALTH AND HUMAN SERVICES AGENCY

Diana S. Dooley
Secretary

May 24, 2017
Date

ATTACHMENT 2

AUTHORIZED DATA EXCHANGE SYSTEM(S)

Attachment 2

Authorized Data Exchange System(s)

BEER (Beneficiary Earnings Exchange Record): Employer data for the last calendar year.

BENDEX (Beneficiary and Earnings Data Exchange): Primary source for Title II eligibility, benefit and demographic data.

LIS (Low-Income Subsidy): Data from the Low-Income Subsidy Application for Medicare Part D beneficiaries -- used for Medicare Savings Programs (MSP).

Medicare 1144 (Outreach): Lists of individuals on SSA roles, who may be eligible for medical assistance for: payment of the cost of Medicare cost-sharing under the Medicaid program pursuant to Sections 1902(a)(10)(E) and 1933 of the Act; transitional assistance under Section 1860D-31(f) of the Act; or premiums and cost-sharing subsidies for low-income individuals under Section 1860D-14 of the Act.

PUPS (Prisoner Update Processing System): Confinement data received from over 2000 state and local institutions (such as jails, prisons, or other penal institutions or correctional facilities) -- PUPS matches the received data with the MBR and SSR benefit data and generates alerts for review/action.

QUARTERS OF COVERAGE (QC): Quarters of Coverage data as assigned and described under Title II of the Act -- The term "quarters of coverage" is also referred to as "credits" or “Social Security credits” in various SSA public information documents, as well as to refer to "qualifying quarters" to determine entitlement to receive Food Stamps.

SDX (SSI State Data Exchange): Primary source of Title XVI eligibility, benefit and demographic data as well as data for Title VIII Special Veterans Benefits (SVB).

SOLQ/SOLQ-I (State On-line Query/State On-line Query-Internet): A real-time online system that provides SSN verification and MBR and SSR benefit data similar to data provided through SVES.

Attachment 2

SVES (State Verification and Exchange System): A batch system that provides SSN verification, MBR benefit information, and SSR information through a uniform data response based on authorized user-initiated queries. The SVES types are divided into five different responses as follows:

SVES I:	This batch provides strictly SSN verification.
SVES I/Citizenship*	This batch provides strictly SSN verification and citizenship data.
SVES II:	This batch provides strictly SSN verification and MBR benefit information
SVES III:	This batch provides strictly SSN verification and SSR/SVB.
SVES IV:	This batch provides SSN verification, MBR benefit information, and SSR/SVB information, which represents all available SVES data.

** Citizenship status data disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 is only for the purpose of determining entitlement to Medicaid and CHIP program for new applicants.*

ATTACHMENT 3

SYSTEM SECURITY REQUIREMENTS THROUGH THE ICON SYSTEM

Not Applicable

Attachment 3

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

12/9/2016

Systems Security Requirements for SWA Access to SSA Information Through the ICON System

A. General Systems Security Standards

SWA's that request and receive information from SSA through the ICON system must comply with the following general systems security standards concerning access to and control of SSA information. The SWA must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA must be stored in a manner that is physically and electronically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information must be processed under the immediate supervision and control of authorized personnel. The SWA must employ both physical and electronic safeguards to ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and State laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the SWA.

B. System Security Requirements for SWA's

SWA's that receive SSA information through the ICON system must comply with the following systems security requirements which must be met before DOL will approve a request from an SWA for online access to SSA information through the ICON system. The SWA system security design and procedures must conform to these requirements. They must be documented by the SWA and subsequently certified by either DOL or by an Independent Verification and Validation (IV&V) contractor prior to initiating transactions to and from SSA through the ICON.

No specific format for submitting this documentation to DOL is required. However, regardless of how it is presented, the information should be submitted to DOL in both hardcopy and electronic format, and the hardcopy should be submitted over the signature of an official representative of the SWA. Written documentation should address each of the following security control areas:

1. General System Security Design and Operating Environment

The SWA must provide a written description of its' system configuration and security features. This should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access controls; and

b. A description of how SSA information will be obtained by and presented to SWA users, including sample computer screen presentation formats and an explanation of whether the SWA system will request information from SSA by means of systems generated or user initiated transactions; and

c. A description of the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to SSA data within the SWA system and an explanation of their job descriptions.

Meeting this Requirement

SWA's must explain in their documentation the overall design and security features of their system. During onsite certification, the IV&V contractor, or other certifier, will use the SWA's design documentation and discussion of the additional systems security requirements (following) as their guide for conducting the onsite certification and for verifying that the SWA systems and procedures conform to SSA requirements.

Following submission to the DOL in connection with the initial certification process, the documentation must be updated any time significant architectural changes are made to the system or to its' security features. During its future compliance reviews (see below), the SSA will ask to review the updated design documentation as needed.

2. Automated Audit Trail

SWA's receiving SSA information through the ICON system must implement and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the SWA client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored

in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This requirement must be met before DOL will approve the SWA's request for access to SSA information through the ICON system.

If SSA-supplied information is retained in the SWA system, or if certain data elements within the SWA system will indicate to users that the information has been verified by SSA, the SWA system also must capture an audit trail record of any user who views SSA information stored within the SWA system. The audit trail requirements for these inquiry transactions are the same as those outlined above for SWA transactions requesting information directly from SSA.

Meeting this Requirement

The SWA must include in their documentation a description of their audit trail capability and a discussion of how it conforms to SSA's requirements. During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the system's audit trail and retrieval capability. The SWA must be able to identify employee's who initiate online requests for SSA information (or, for systems generated transaction designs, the SWA case that triggered the transaction), the time and date of the request, and the purpose for which the transaction was originated. The certifier, or IV&V contractor, also will request a demonstration of the system's audit trail capability for tracking the activity of SWA employees that are permitted to view SSA supplied information within the SWA system, if applicable.

During its future compliance reviews (see below), the SSA also will test the SWA audit trail capability by requesting verification of a sample of transactions it has processed from the SWA after implementation of access to SSA information through the ICON system.

3. System Access Control

The SWA must utilize and maintain technological (logical) access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The SWA must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The SWA must have

management control and oversight of the function of authorizing individual user access to SSA information, and over the process of issuing and maintaining access control PINs and passwords for access to the SWA system.

Meeting this Requirement

The SWA must include in their documentation a description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions to verify their responsibilities in the SWA's access control process and will observe a demonstration of the procedures for logging onto the SWA system and for accessing SSA information.

4. **Monitoring and Anomaly Detection**

The SWA's system must include the capability to prevent employees from browsing (i.e. unauthorized access or use of SSA information) SSA records for information not related to an SWA client case (e.g. celebrities, SWA employees, relatives, etc.) If the SWA system design is transaction driven (i.e. employees cannot initiate transactions themselves, rather, the SWA system triggers the transaction to SSA), or if the design includes a "permission module" (i.e. the transaction requesting information from SSA cannot be triggered by an SWA employee unless the SWA system contains a record containing the client's Social Security Number), then the SWA needs only minimal additional monitoring and anomaly detection. If such designs are used, the SWA only needs to monitor any attempts by their employees to obtain information from SSA for clients not in their client system, or attempts to gain access to SSA data within the SWA system by employees not authorized to have access to such information.

If the SWA design does not include either of the security control features described above, then the SWA must develop and implement compensating security controls to prevent their employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of queries requested by individual SWA employees, and systematic or manual procedures for verifying that requests for SSA information are in compliance with valid official business purposes. The SWA system must produce reports providing SWA management and/or supervisors with the capability to appropriately monitor user activity, such as:

- User ID exception reports

This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system or to the transaction that initiates requests for information from SSA, including failed attempts to enter a password.

- Inquiry match exception reports

This type of report captures information about users who may be initiating transactions for Social Security Numbers that have no client case association within the SWA system.

- System error exception reports

This type of report captures information about users who may not understand or be following proper procedures for access to SSA information through the ICON system.

- Inquiry activity statistical reports

This type of report captures information about transaction usage patterns among authorized users, which would provide SWA management a tool for monitoring typical usage patterns compared to extraordinary usage.

The SWA must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors, or to local security officers, to ensure that the reports are used by those whose responsibilities include monitoring the work of the authorized users.

Meeting this Requirement

The SWA must explain in their documentation how their system design will monitor and/or prevent their employees from browsing SSA information. If the design is based on a "permission module" (see above), a similar design, or is transaction driven (i.e. no employee initiated transactions) then the SWA does not need to implement additional systematic and/or managerial oversight procedures to monitor their employees access to SSA information. The SWA only needs to monitor user access control violations. The documentation should clearly explain how the system design will prevent SWA employees from browsing SSA records.

If the SWA system design permits employee initiated transactions that are uncontrolled (i.e. no systematically enforced relationship to an SWA client), then the SWA must develop and document the monitoring and anomaly detection process they will employ to deter their employees from browsing SSA

information. The SWA should include sample report formats demonstrating their capability to produce the types of reports described above, and the SWA should include a description of the process that will be used to distribute these reports to managers/supervisors, and the management controls that will ensure the reports are used for their intended purpose.

During onsite certification, the IV&V contractor, or other certifier, will request a demonstration of the SWA's monitoring and anomaly detection capability.

- If the design is based on a permission module or similar design, or is transaction driven, the SWA will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the SWA will demonstrate the process by which requests for SSA information are prevented for Social Security Numbers not present in the SWA system (e.g. by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the SWA system.)

- If the design is based on systematic and/or managerial monitoring and oversight, the SWA will provide copies of anomaly detection reports and demonstrate the report production capability.

During onsite certification, the IV&V contractor, or other certifier, also will meet with a sample of managers and/or supervisors responsible for monitoring ongoing compliance to assess their level of training to monitor their employee's use of SSA information, and for reviewing reports and taking necessary action.

5. **Management Oversight and Quality Assurance**

The SWA must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA information through the ICON system, and to ensure there is ongoing compliance with the terms of the SWA's data exchange agreement with SSA. The management oversight function must consist of one or more SWA management officials whose job functions include responsibility for assuring that access to and use of SSA information is appropriate for each employee position type for which access is granted.

This function also should include responsibility for assuring that employees granted access to SSA information receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online access to SSA information. In addition, there should be the capability to randomly sample work activity involving online requests for SSA information to

determine whether the requests comply with these guidelines. These functions should be performed by SWA employees whose job functions are separate from those who request or use information from SSA.

Meeting this Requirement

The SWA must document that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information, and oversight and monitoring of the use of SSA information within the SWA business process. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individual(s) responsible for these functions and request a description of how these responsibilities will be carried out.

6. **Security Awareness and Employee Sanctions**

The SWA must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other Federal and State laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Requirement

The SWA must document that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of SSA information. The SWA should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures, training material and employee acknowledgment statements.

During onsite certification, the IV&V contractor, or other certifier, will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out. The IV&V contractor, or other certifier, also will meet with a sample of SWA employees to assess their level of training and

understanding of the requirements and potential sanctions applicable to the use and misuse of SSA information.

7. Data and Communications Security

The encryption method employed must meet acceptable standards designated by the National Institute of Standards and Technology (NIST). The recommended encryption method to secure data in transport for use by SSA is the Advanced Encryption Standard (AES) or triple DES (DES3) if AES is unavailable.

D. Onsite Systems Security Certification Review

The SWA must obtain and participate in an onsite review and compliance certification of their security infrastructure and implementation of these security requirements prior to being permitted to submit online transaction to SSA through the ICON system. DOL will require an initial onsite systems security certification review to be performed by either an independent IV&V contractor, or other DOL approved certifier. The onsite certification will address each of the requirements described above and will include, where appropriate, a demonstration of the SWA's implementation of each requirement. The review will include a walkthrough of the SWA's data center to observe and document physical security safeguards, a demonstration of the SWA's implementation of online access to SSA information through the ICON system, and discussions with managers/supervisors. The IV&V contractor, or other certifier, also will visit at least one of the SWA's field offices to discuss the online access to SSA information with a sample of line workers and managers to assess their level of training and understanding of the proper use and protection of SSA information.

The IV&V contractor, or other certifier, will separately document and certify SWA compliance with each SSA security requirement. To fully comply with SSA's security requirements and be certified to connect to SSA through the ICON system, the SWA must submit to DOL a complete package of documentation as described above and a complete certification from an independent IV&V contractor, or other DOL approved certifier, that the SWA system design and infrastructure is in agreement with the SWA documentation and consistent with SSA requirements. Any unresolved or unimplemented security control features must be resolved by the SWA before DOL will authorize their connection to SSA through the ICON system.

Following initial certification and authorization from DOL to connect to SSA through the ICON system, SSA is responsible for future systems security compliance reviews. SSA conducts such reviews approximately once every three years, or as needed if there is a significant change in the SWA's computing platform, or if there is a violation of any of SSA's systems security requirements or an unauthorized disclosure of SSA information by the SWA. The format of those reviews generally consists of

reviewing and updating the SWA compliance with the systems security requirements described above.

SENSITIVE DOCUMENT

ATTACHMENT 4

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS

AND PROCEDURES

(Technical Systems Security Requirements- TSSR)

ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SOCIAL SECURITY ADMINISTRATION

SENSITIVE DOCUMENT

Version 7.0
July 2015

TABLE OF CONTENTS

1. Introduction

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its ***Electronic Information Exchange Partners (EIEPs)***. EIEPs must protect the information with efficient and effective security controls. EIEPs are entities that have electronic information exchange agreements with the agency.

This document consistently references the concept of **Electronic Information Exchange Partners (EIEP)**; however, our **Compliance Review Questionnaire (CRQ)** and **Security Design Plan (SDP)** documents will use the terms "**state agency"** or "**state agency, contractor(s), and agent(s)"** for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms "state agency" or "state agency, contractor(s), and agent(s)" in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to our data exchange agreements between state agencies and SSA. It will also provide a more "user-friendly" experience for the state officials who complete these forms on behalf of their state agencies.

The objective of this document is twofold. The first is to ensure that SSA can properly certify EIEPs as compliant with SSA security standards, requirements, and procedures. The second is to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document helps EIEPs understand the criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information. Finally, this document provides the framework and general procedures for SSA's Security Certification and Compliance Review Programs.

The primary statutory authority that supports the information contained in this document is the **Federal Information Security Management Act (FISMA)**. FISMA became law as part of the **Electronic Government Act of 2002.** FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the **National Institute of Standards and Technology (NIST)**, a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA's requirements mirror the NIST-defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

To gain electronic access to SSA-provided information, under the auspices of a data exchange agreement, EIEP's must comply with SSA's most current **Technical System Security Requirements (**hereafter referred to as **TSSRs)** to gain access to SSA-provided information. This document is **synonymous** with the **Electronic Information Exchange Security Requirements and Procedures for State and**

Local Agencies Exchanging Electronic Information with the Social Security Administration in the agreements. The TSSR specifies minimally acceptable levels of security standards and controls to protect SSA-provided information. SSA maintains the TSSR as a living document—subject to change--that addresses emerging threats, new attack methods and the development of new technology that potentially places SSA-provided information at risk. EIEPs may proactively ensure their ongoing compliance to the TSSR by periodically requesting the most current version from SSA. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. SSA refers to this process as **Gap Analysis**. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement.

SSA's standard for categorization of information (Moderate) and information systems is to provide appropriate levels of security according to risk level. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry.

2. Electronic Information Exchange (EIE) Definition

For discussion purposes herein, EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes direct terminal access (DTA) to SSA systems, batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

3. Roles and Responsibilities

The SSA ***Office of Information Security (OIS)*** has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic data exchange agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of the electronic data exchange

agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure initial security certifications and triennial security compliance reviews. This includes (but not limited to) any EIEP that processes, maintains, transmits, or stores SSA-provided information in accordance with pertinent Federal requirements.

a. The SSA Regional ***Data Exchange Coordinators*** (DECs) serve as a bridge between SSA and EIEPs. DECs assist in coordinating data exchange security review activities with EIEPs; (e.g., providing points of contact with state agencies, assisting in setting up security reviews, etc.) DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or agent becomes aware of suspected or actual loss of SSA-provided information.

b. SSA requires **EIEPs** to adhere to the standards, requirements, and procedures, published in this TSSR document.

   - "Personally Identifiable Information (PII)," covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual's identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or lined to a specific individual's medical, educational, financial, and employment information.

   - The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not "PII" as defined by the Act.

   - Both SSA and EIEPs must remain diligent in the responsibility for establishing *appropriate* management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.

c. A State Transmission/Transfer Component (STC) is an organization that performs as an electronic information conduit or collection point for one of more other entities (also referred to as a hub). An STC must also adhere to the same management, operational and technical controls as SSA and the EIEP.

NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding

safeguards for protecting FTI, consult IRS Publication 1075, **Tax Information Security Guidelines for Federal, State, and Local Agencies.**

4. General Systems Security Standards

EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA.

1. EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP"s ability to:

    - safeguard the information in conformance with SSA requirements
    - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information
    - detect instances of misuse or abuse of SSA-provided information

For example, Utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.

2. The EIEP must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.
3. The EIEP must use the software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.
4. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.
5. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.
6. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

    NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section 'Contractors of Electronic Information Exchange Partners in the Systems Security Requirements for additional information.

7. EIEPs must store information received from SSA in a manner that, at all times, is

physically and electronically secure from access by unauthorized persons.

8. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.

9. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.

10. EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.

11. EIEPs must have an active and robust security awareness program, which is mandatory for all employees who access SSA-provided information.

12. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.

13. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency plan that includes a disaster recovery plan that addresses both natural disaster and cyber-attack situations.

14. SSA requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.

15. At its discretion, SSA or its designee must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5. Systems Security Requirements

5.1 Overview

SSA's TSSR represent the current industry standard for security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA, through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The TSSR address management, operational, and technical controls regarding security safeguards to ensure only authorized disclosure and usage of SSA provided information used, maintained, transmitted, or stored by SSA's EIEPs. SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege."

SSA requires EIEPs to document and notify SSA prior to sharing SSA-provided information with another state entity, or to allow them direct access to their system. **This includes (but not limited to) law enforcement, other state agencies, and state organizations that perform audit, quality, or integrity functions**.

SSA recommends that the EIEP develop and publish a comprehensive Information Technology (IT) Systems Security Policy document that specifically addresses:

1) the classification of information processed and stored within the network,

2) management, operational, and technical controls to protect the information stored and processed within the network,

3) access to the various systems and subsystems within the network,

4) Security Awareness Training,

5) Employee and End User Sanctions Policy,
6) Contingency Planning and Disaster Recovery

7) Incident Response Policy, and

8) The disposal of protected information and sensitive documents derived from the system or subsystems on the network.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.2 General System Security Design and Operating Environment *(Planning (PL) Family – (System Security Plan), Contingency Plan (CP) Family, Physical and Environmental (PE) Family, NIST SP 800-53 rev. 4)*

In accordance with the NIST suite of Special Publications (SP) (e.g., 800-53, 800-34, etc.), SSA requires the EIEP to maintain policies, procedures, descriptions, and explanations of their overall system design, configuration, security features, and operational environment. They should include explanations of how they conform to SSA's TSSRs. The EIEPs General System Security design and Operating Environment must also address:

a) the operating environment(s) in which the EIEP will utilize, maintain, store, and transmit SSA-provided information,

b) the business process(es) in which the EIEP will use SSA-provided information,

c) the physical safeguards employed to ensure that unauthorized personnel, the public or visitors to the agency cannot access SSA-provided information,

d) details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available,

e) electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest ,

f) a senior management approved Information System Contingency Plan (ISCP) that addresses both internal and external threats. SSA requires the ISCP to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that addresses the security of SSA-provided information if a disaster occurs. SSA recommends that state agencies perform disaster exercises at least once annually.,

g) how the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means; including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.)

h) how the configurations of devices (e.g., servers, workstations, portable devices) involving SSA-provided information complies with recognized industry standards (i.e. NIST SP's) and SSA's TSSR, and

i) organizational structure of the agency, number of users, and all external entities that will have access to the system and/or application that displays, transmits, and/or application that displays, transmits and/or stores SSA-provided information.

Note: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information we provide.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.3 System Access Control
(Access Control (AC) Family, NIST SP 800-53 rev. 4)

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user-access security software package (e.g.,RAC-F, ACF-2, TOP SECRET, Active Directory, etc.) or a security software design, which is equivalent to such products. The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) SmartCard/biometric identifier, etc., (for authenticating users), (and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

The EIEP's password policies must require stringent password construction as supported by current NIST guidelines for the user accounts of persons, processes, or devices whose functions require access privileges above those of ordinary users. **SSA strongly recommends Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must require stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and/or special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

In addition, SSA has the following specific requirements in the area of Access Control:

1. Upon hiring or before granting access to SSA-provided information, EIEPs should verify the identities of any employees, contractors, and agents who will have access to SSA-provided information in accordance with the applicable agency or state's "personnel identity verification policy."

2. SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information, in accordance with NIST guidelines. SSA recommends no fewer than three (3) and no greater than five (5)..

3. SSA requires that the state agency designate specific official(s) or functional component(s) to issue PINs, passwords, biometric identifiers, or Personal Identity Verification (PIV) credentials to individuals who will access SSA-provided information. **SSA also requires that the state agency prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.**

4. SSA requires that EIEPs grant access to SSA-provided information based on least privilege, need-to-know, and separation of duties. State agencies should not routinely grant employees, contractors, or agents access privileges that exceed the organization's business needs. SSA also requires that EIEPs periodically review employees, contractors, and agent's system access to determine if the same levels and types of access remain applicable.

5. If an EIEP employee, contractor, or agent is subject to an adverse administrative action by the EIEP (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the EIEP remove his or her access to SSA-provided information in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA-provided information.

6. SSA requires that work-at-home, remote access, and/or Internet access comply with applicable Federal and state security policy and standards. Furthermore, the EIEPs access control policy must define the safeguards in place to adequately protect SSA-provided information for work-at-home, remote access, and/or Internet access.

7. SSA requires EIEPs to design their system with logical control(s) that prevent unauthorized browsing of SSA-provided information. SSA refers to this setup as a **Permission Module**. The term "**Permission Module**" supports a business rule and systematic control that prevents users from browsing a system that contains SSA-provided information. It also supports the principle of **referential integrity**. It should prevent non-business related or unofficial access to SSA-provided information. Before a user or process requests SSA-provided information for verification, the system should verify it is an authorized transaction. Some organizations use the term "referential integrity" to describe the verification step. A properly configured Permission Module should prevent a user from performing any actions not consistent with a need-to-know business process. If a logical permission module configuration is not possible, the state agency must enforce its Access Control List (ACL) in accordance with the principle of least privilege. **The only acceptable compensating control for a system that lacks a permission module is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.4 Automated Audit Trail

(Audit and Accountability (AU) Family, NIST SP 800-53 rev. 4)

SSA requires EIEPs, and other STCs or agencies that provide audit trail services to other state agencies that receive information electronically from SSA, to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and (efficiently) retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The ATS must create transaction files to capture all input from interactive internet applications that access or query SSA-provided information.

SSA requires that the agency's ATS create an audit record when users view screens that contain SSA-provided information. If an STC handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet NIST's guidelines for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

SSA requires that EIEPs have automated retrieval and collection of audit records. Such automated functions can be via online queries, automated reports, batch processing, or any other logical means of delivering audit records in an expeditious manner. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request.

Access to the audit file must be restricted to authorized users with a "need to know," audit file data must be unalterable (read-only), and maintained for a minimum of three (3) (preferably seven (7)) years. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request. The EIEP must backup audit trail records on a regular basis to ensure its availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files to ensure the integrity of the data.

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicates to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who view SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical. **Similar to the Permission Module requirement above, the only acceptable compensating control for a system that lacks an Automated Audit Trail System (ATS) is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.5 Personally Identifiable Information (PII)

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and AP Family – Authority and Purpose (Privacy Controls), NIST SP 800-53 rev. 4)

Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal or identifying information linked or linkable to a specific individual. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines ***a PII loss*** as a circumstance when an EIEP employee, contractor, or agent has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident. SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA-provided information.

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to ***Incident Reporting***).

The EIEP should have procedural documents to describe methods and controls for safeguarding SSA-provided PII while in use, at rest, during transmission, or after archiving. The document should explain how the EIEP manages and handles SSA-provided information on print media and explain how the methods and controls conform to NIST requirements. SSA requires that printed items that contain SSA-provided PII always remain in the custody of authorized EIEP employees, contractors, or agents. SSA also requires that the agency destroy the items when no longer required for the EIEP's business process. If retained in paper files for evidentiary purposes, the EIEP should safeguard such PII in a manner that prevents unauthorized personnel from accessing such materials. All agencies that receive SSA-provided information must maintain an inventory of all documents that outline statewide or agency policy and procedures regarding the same.

5.6 Monitoring and Anomaly Detection

(Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137, E-Government Act of 2002 (P.L. 107-347), and Security Assessment and Authorization (CA) and Risk Assessment (RA) Families, NIST SP 800-53 rev. 4)

SSA requires that the EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS). The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

1) the EIEP's security controls continue to be effective over time,

2) the EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection,

3) only authorized individuals, devices, and processes have access to SSA-provided information,

4) the EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (e.g., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur,

5) the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes,

6) upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk,

7) in the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions, and

8) trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

The EIEP's system must include the capability to prevent users from unauthorized browsing of SSA records. SSA requires the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they also must have anomaly detection to monitor an employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a manner that it goes undetected. The SSA permission module design employs both role and rules based logical access control restrictions. (Refer to ***Access Control***)

If the EIEP's design ***does not use*** a permission module ***and*** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, such as: systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes.

Risk Management Program

SSA recommends that EIEPs develop and maintain a published Risk Assessment Policy and Procedures document. A Risk Management Program may include, but is not limited to the following:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance,

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls,

3. A function that conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits,

4. An independent function that conducts vulnerability and risk assessments, reviews risk assessment results, and disseminates such information to senior management,

5. A firm commitment from senior management to update the risk assessment whenever there are significant changes to the information

system or environment of operation or other conditions that may affect the security of SSA-provided information,

6. A robust vulnerability scanning protocol that employs industry standard scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process,

7. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk, and

8. Shares information obtained from the vulnerability scanning process and security control assessments with senior management to help eliminate similar vulnerabilities in other information systems that receive, process, transmit, or store SSA-provided information.

Note: The EIEP's decision to initiate or maintain an official Risk Management Program and establish a formal Risk Assessment Strategy for mitigating risk is strictly voluntary, but highly recommended by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.7 Management Oversight and Quality Assurance

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the AC – Access Control & PM – Program Management Families, NIST SP 800-53 rev. 4)

SSA requires the EIEP to establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized users have access to SSA-provided information. This will ensure there is ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the TSSRs established for access to SSA-provided information. The entity responsible for management oversight should consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate users and position types (least privilege), which require the SSA-provided information to do their jobs (need-to-know).

SSA requires the EIEP to ensure that users granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the civil and criminal consequences or penalties for misuse or improper disclosure.

SSA requires that EIEPs establish the following job functions and require that only users whose job functions are separate from personnel who request or use SSA-provided information.

SSA requires that EIEPs establish the following job functions separate from personnel who request or use SSA-provided information.

a) Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.

b) Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements

SSA requires the EIEP's system to produce reports that allow management and/or supervisors to monitor user activity. The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

1. **User ID Exception Reports:**

   This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to a transaction that initiates requests for information from SSA, including failed attempts to enter a password.

2. **Inquiry Match Exception Reports:**

   This type of report captures information about users who initiate transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management must review 100% of these cases).**

3. **System Error Exception Reports:**

   This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

4. **Inquiry Activity Statistical Reports:**

   This type of report captures information about transaction usage patterns among authorized users and is a tool that enables the EIEP's management to monitor typical usage patterns in contrast to extraordinary usage patterns.

The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.8 Data and Communications Security

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Access Control (AC), Configuration Management (CM), Media Protection (MP), and System and Communication (SC) Families, NIST SP 800-53 rev. 4)

SSA requires EIEPs to encrypt PII and SSA-provided information when transmitting across dedicated communications circuits between its systems, intrastate communications between its local office locations, and on the EIEP's mobile computers, devices and removable media. The EIEP's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or Triple DES (Data Encryption Standard 3). **Files encrypted for external users (when using tools such as Microsoft Word encryption,) require a key length of at least nine characters.** SSA recommends that the key (also referred to as a password) contain both special characters and numbers. SSA supports the NIST Guidelines that requires the EIEP deliver the key so that it does not accompany the media. The EIEP must secure the key when not in use or unattended.

SSA discourages the use of the public Internet for transmission of SSA-provided information. If, however, the EIEP uses the public Internet or other electronic communications, such as emails and faxes to transmit SSA-provided information, they must use a secure encryption protocol such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSA also recommends 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. The EIEP should only send data to a secure address or device to which the EIEP can control and limit access to only specifically authorized individuals and/or processes. **SSA recommends that EIEPs use Media Access Control (MAC) Filtering and Firewalls to protect access points from unauthorized devices attempting to connect to the network.**

EIEPs should not retain SSA-provided information any longer than business purpose(s) dictate. The IEA with SSA stipulates a time for data retention. The EIEP should delete, purge, destroy, or return SSA-provided information when the business purpose for retention no longer exists.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may apply specific SSA-provided information to the EIEP's matched record from a preexisting data source. Federal law prohibits duplication and redisclosure of SSA-provided information without written approval from SSA.

This prohibition applies to both internal and external sources who do not have a "need-to-know." SSA recommends that EIEPs use either **Trusted Platform Module (TPM)** or **Hardware Security Module (HSM)** technology solutions to encrypt data at rest on hard drives and other data storage media.

SSA requires EIEPs to prevent unauthorized disclosure of SSA-provided information after they complete processing and after the EIEP no longer requires the information. The EIEP's operational processes must ensure that no residual SSA-provided information remains on the hard drives of user's workstations after the user exits the application(s) that use SSA-provided information. If the EIEP must send a computer, hard drive, or other computing or storage device offsite for repair, the EIEP must have a non-disclosure clause in their contract with the vendor. If the EIEP used the item in connection with a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the EIEP's vendor contract. The EIEP must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the EIEP to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

To sanitize media, the EIEP should use one of the following methods:

1. **Overwriting/Clearing:**

   Overwrite utilities can only be used on working devices. Overwriting is appropriate only for devices designed for multiple reads and writes. The EIEP should overwrite disk drives, magnetic tapes, floppy disks, USB flash drives, and other rewriteable media. The overwrite utility must completely overwrite the media. SSA recommends the use of ***purging*** media sanitization to make the data irretrievable, protecting data against laboratory attacks or forensics. Reformatting the media does not overwrite the data.

2. **Degaussing:**

   Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic media (e.g., optical discs). SSA and NIST Guidelines require EIEP to use a certified tool designed to degauss each particular type of media. NIST guidelines require certification of the tool to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures.

3. Physical destruction:

NIST guidelines require physical destruction when degaussing or over-writing cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drives, etc.). Examples of physical destruction include shredding, pulverizing, and burning.

State agencies may retain SSA-provided information in hardcopy only if required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agency's retention of records. The EIEP must control print media containing SSA-provided information to restrict access to authorized employees who need such access to perform official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when no longer required for business purposes. SSA requires the EIEP to destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

State agencies may use any accretions, deletions, or changes to the SSA-provided information governed by the CMPPA agreement to update their master files or federally funded state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

NOTE: Hand tearing or lining through documents to obscure information does not meet SSA's requirements for appropriate destruction of PII.

The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.

Special Note regarding Cloud Service Providers:

If the EIEP will store SSA-provided information through a Cloud Service Provider, please provide the name and address of the cloud provider. Describe the security responsibilities the contract requires to protect SSA-provided information.

SSA will ask for detailed descriptions of the security features contractually required of the cloud provider and information regarding how they will protect SSA-provided information at rest and when in transit.

EIEPs cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.9 Incident Reporting

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Incident Response (IR) Family, NIST SP 800-53 rev. 4)

FISMA, NIST Guidelines, and Federal Law require the EIEP to develop and implement policies and procedures to respond to potential data breaches or PII loses. EIEPs must articulate, in writing, how the policies and procedures conform to SSA's requirements. The procedures must include the following information:

> *If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact* ***within one hour****, the responsible State Agency official or delegate must report the incident by contacting* ***SSA's National Network Service Center (NNSC) toll free at 877-697-4889*** *(select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. **SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, contractors, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or PII loss.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.10 Security Awareness Training and User Sanctions

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The EIEP must have an active and robust security awareness program and security training for all employees, contractors, and agents who access SSA-provided information. The training and awareness programs must include:

a. the sensitivity of SSA-provided information and addresses the Privacy Act and other Federal and state laws governing its use and misuse,

b. the rules of behavior concerning use and security in systems and/or applications processing SSA-provided information,

c. the restrictions on viewing and/or copying SSA-provided information,

d. the responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information,

e. the proper disposal of SSA-provided information,

f. the security breach and data loss incident reporting procedures,

g. the basic understanding of procedures to protect the network from malware attacks,

h. spoofing, phishing and pharming, and network fraud prevention, and

i. the possible criminal and civil sanctions and penalties for misuse of SSA-provided information.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

SSA requires the EIEP to provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, or agent who views SSA-provided information also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure. SSA requires the state agency to require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. The non-disclosure attestation must also include acknowledgement from each employee, contractor, and agent that he or she understands and accepts the potential criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information. The state agency must retain the non-disclosure attestations for at least five (5) to seven (7) years for each individual who processes, views, or encounters SSA-provided information as part of their duties.

SSA strongly recommends the use of login banners, emails, posters, signs, memoranda, special events, and other promotional materials to encourage security awareness throughout your enterprise.

The state agency must designate a department or party to take the responsibility to provide ongoing security awareness training for all employees, contractors, and agents who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee, contractor, and agent's responsibility for proper use and protection of SSA-provided information
- Proper disposal of SSA-provided information
- Security incident reporting procedures
- Basic understanding of procedures to protect the network from malware attacks

- Spoofing, Phishing and Pharming scam prevention
- The possible sanctions and penalties for misuse of SSA-provided information

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.11 Contractors of Electronic Information Exchange Partners

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Risk Assessment (RA), System and Services Acquisition (SA), Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

The state agency's employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by the Agreement may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. The state agency will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

Contractors of the state agency must adhere to the same security requirements as employees of the state agency. The state agency is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The state agency must enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties. Such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the state agency's agreement with SSA.

The state agency must provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of their duties. If the contractor processes, handles, or transmits information provided to the state agency by SSA or has authority to perform on the state agency's behalf, the state agency should clearly state the specific roles and functions of the contractor within the agreement. The state agency will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA-provided information.

The state agency must also require that contractors and agents who will process, handle, or transmit information provided to the state agency by SSA to include language in their signed agreement that obligates the contractor to follow the terms of the state agency's data exchange agreement with SSA. The state agency must also make certain that the contractor and agent's employees receive the same security awareness training as the state agency's employees. The state agency, the contractor, and the agent should maintain awareness-training records for their employees and require the same mandatory annual

certification procedures.

SSA requires the state agency to subject the contractor to ongoing security compliance reviews that must meet SSA standards. The state agency will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA. The state agencies will provide SSA with documentation of their recurring compliance reviews of their contractors and agents. The state agencies will provide the documentation to SSA during their scheduled compliance and certification reviews or upon SSA's request.

If the state agency's contractor will be involved with the processing, handling, or transmission of information provided to the EIEP by SSA offsite from the EIEP, the EIEP must have the contractual option to perform onsite reviews of that offsite facility to ensure that the following meet SSA's requirements:

a) safeguards for sensitive information,

b) technological safeguards on computer(s) that have access to SSA-provided information,

c) security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information, and

d) continuous monitoring of the EIEP contractors or agent's network infrastructures and assets.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners

(NIST SP 800-144, NIST SP 800-145, NIST SP 800-146, OMB Memo M-14-03, NIST SP 137)

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." The three service models, as defined by NIST SP 800-145 are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Furthermore, The Federal Risk and Authorization Program (FedRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

SSA requires the State Agency, contractor(s), and agent(s) to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

SSA requires the State Agency, contractor(s), and agent(s) to agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

SSA requires that the State Agency thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s). If the obligations, services, or conditions widely differ from agency to agency, we require separate SDP Questionnaires to address the CSP services provided to each state agency involved in the receipt, processing, storage, or disposal of SSA-provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6. Security Certification and Compliance Review Programs
(NIST SP 800-18 – System Security Plans and Planning (PL) Family, NIST SP 800-53 rev. 4)

SSA's security certification and compliance review programs are distinct processes. The certification program is a unique episodic process when an EIEP initially requests electronic access to SSA-provided information or makes substantive changes to existing exchange protocol, delivery method, infrastructure, or platform. The certification process entails two stages (refer to 6.1 for details) intended to ensure that management, operational, and technical security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements at the time of certification and satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program entails cyclical security review of the EIEP performed by, or on behalf of SSA. The purpose of the review is to to assess an EIEP's conformance to SSA's current security requirements at the time of the review engagement. The compliance review program applies to both online and batch access to SSA-provided information. Under the compliance review program, EIEPs are subject to ongoing and periodic security reviews by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.1 The Security Certification Program
(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

The security certification process applies to EIEPs that seek online electronic access to SSA-provide information and consists of two general phases:

a) **Phase 1:** The Security Design Plan (SDP) is a formal written plan authored by the EIEP to document its management, operational, and technical security controls to safeguard SSA-provided information (refer to ***Documenting Security Controls in the Security Design Plan)***.

NOTE: **SSA may have legacy EIEPs (EIEPs not certified under the current process) who have not prepared an SDP. SSA strongly recommends that these EIEPs prepare an SDP.**

The EIEP's preparation and maintenance of a current SDP will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's TSSRs, and providing for more efficient security reviews.

b) **Phase 2:** The SSA Onsite Certification is a formal security review conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to ***The Certification Process***).

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.2 Documenting Security Controls in the SDP

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

6.2.1 When an SDP is required:

EIEPs must submit an SDP when one or more of the following circumstances apply:

a) to obtain approval for requested access to SSA-provided information for an initial agreement,

b) to obtain approval to reestablish previously terminated access to SSA-provided information,

c) to obtain approval to implement a new operating or security platform that will involve SSA-provided information,

d) to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent SDP or of their most recent successfully completed security review,

e) to confirm compliance when one or more security breaches or incidents involving SSA-provided information occurred since approval of the EIEP's most recent SDP or of their most recent successfully completed security review,

f) to document descriptions and explanations of measures implemented as the result of a data breach or security incident,

g) to document descriptions and explanations of measures implemented to resolve non-compliancy issue(s), and

h) to obtain a new approval after SSA revoked approval of the most recent SDP

SSA may require a new SDP if changes occurred (other than those listed above) that may affect the terms of the EIEP's data exchange agreement with SSA.

SSA will not approve the SDP or allow the initiation of transactions and/or access to SSA-provided information before the EIEP complies with the TSSRs.

NOTE: EIEPs that function only as an STC, transferring SSA-provided information to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA-provided information. **(See Page 48 Definition of STC)**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.3 The Certification Process
(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review is to ensure the EIEP's management, operational, and technical controls safeguarding SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request the EIEP to participate in an onsite review and compliance certification of their security infrastructure.

The onsite review may address any or all of SSA's security requirements and include, when appropriate:

1) a demonstration of the EIEP's implementation of each security requirement,

2) a physical review of pertinent supporting documentation to verify the accuracy of responses in the SDP,

3) a demonstration of the functionality of the software interface for the system that will receive, process, and store SSA-provided information,

4) a demonstration of the Automated Audit Trail System (ATS),

5) a walkthrough of the EIEP's data center to observe and document physical security safeguards,

6) a demonstration of the EIEP's implementation of electronic exchange of data with SSA,

7) a discussions with managers, supervisors, information security officers, system administrators, or other state stakeholders,

8) an examination of management control procedures and reports pertaining to anomaly detection or anomaly prevention,

9) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

10) a demonstration of the permission module or similar design, to show how the system triggers requests for information from SSA,

11) a demonstration of how the process for requests for SSA-provided information prevents SSNs not present in the EIEP's system from sending requests to SSA.

We may attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.

During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's ATS and its record retrieval capability. SSA or a certifier may request a demonstration of the ATS' capability to track the activity of employees who have the potential to access SSA-provided information within the EIEP's system. The certifier may request more information from those EIEPs who use an STC to handle and audit transactions. SSA or a certifier may conduct a demonstration to see how the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

If an STC handles and audits an EIEP's transactions, SSA requires the EIEP to demonstrate both their in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor or agent who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include the contractor's facility in the onsite certification review. The inspection may occur with or without a representative of the EIEP.

Upon successful completion of the onsite certification review, SSA will authorize electronic access to production data by the EIEP. SSA will provide written notification of its certification to the EIEP and all appropriate internal SSA components.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.5 The Compliance Review Program and Process
(NIST SP 800-18 – System Security Plans, Configuration Management (CM), Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

Similar to the certification process, the compliance review program entails a process intended to ensure that EIEPs that receive electronic information from SSA are in full compliance with the SSA's TSSRs. SSA requires EIEPs to complete and submit (based on a timeline agreed upon by SSA and EIEP's stakeholders) a Compliance Review Questionnaire (CRQ). The CRQ (similar to the SDP), describes the EIEP's management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure. We also want to verify that those safeguards function and work as intended.

As a practice, SSA attempts to conduct compliance reviews following a 3-5 year periodic review schedule. However, as circumstances warrant, a review may take place at any time. Three prominent examples that would trigger an ad hoc review are:

A. a significant change in the outside EIEP's computing platform,

B. a violation of any of SSA's TSSRs, or

C. an unauthorized disclosure of SSA-provided information by the EIEP.

SSA may conduct onsite compliance reviews and include both the EIEP's main facility and a field office.

SSA may, at its discretion, request that the EIEP participate in an onsite compliance review of their security infrastructure to confirm the implementation of SSA's security requirements.

The onsite review may address any or all of SSA's security requirements and include, where appropriate:

D. a demonstration of the EIEP's implementation of each requirement

E. a random sampling of audit records and transactions submitted to SSA

F. a walkthrough of the EIEP's data center to observe and document physical security safeguards

G. a demonstration of the EIEP's implementation of online exchange of data with SSA,

H. a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,

I. an examination of management control procedures and reports pertaining to anomaly detection and prevention reports,

J. a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

K. a demonstration of how a permission module or similar design triggers requests for information from SSA, and

L. a demonstration of how a permission module prevents the EIEP's system from processing SSNs not present in the EIEP's system.

1) We can accomplish this by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system.

SSA may perform an onsite or remote review for reasons including, but not limited, to the following:

a) the EIEP has experienced a security breach or incident involving SSA-provided information

b) the EIEP has unresolved non-compliancy issue(s)

c) to review an offsite contractor's facility that processes SSA-provided information

d) the EIEP is a legacy organization that has not yet been through SSAs security certification and compliance review programs

e) the EIEP requested that SSA perform an IV & V (Independent Verification and Validation review)

During the compliance review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees who view SSA-provided information within the EIEP's system. The certifier may request EIEPs that have STCs that handle and audit transactions with SSA to demonstrate the process used to obtain audit information from the STC.

If an STC handles and audits the EIEP's transactions with SSA, we may require the EIEP to demonstrate both their in-house audit capabilities and the processes used to

obtain audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will process, handle, or transmit the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. The format of the review in routine circumstances (e.g., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, etc.) will generally consist of reviewing and updating the EIEP's compliance with the systems security requirements described above in this document. At the conclusion of the review, SSA will issue a formal report to appropriate EIEP personnel. The Compliance Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

NOTE: SSA will never request documentation for compliance reviews unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its electronic data exchange agreement with SSA and the associated system security requirements and procedures. SSA will not retain the EIEP's documentation any longer than required. SSA will delete, purge, or destroy the documentation when the retention requirement expires.

Compliance Reviews are either on-site or remote reviews. High-risk reviews must be onsite reviews, medium risk reviews are usually onsite, and low risk reviews may qualify for a remote review via telephone. The past performance of the entire state determines whether a review is onsite or remote **SSA determines a state's risk level based on the "high water mark principle."** If one agency is high risk, the entire state is high risk. The following is a high-level example of the analysis that aids SSA in making a preliminary determination as to which review format is appropriate. SSA may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

A. High/Medium Risk Criteria

1) undocumented closing of prior review finding(s),

2) implementation of management, operational or technical controls that affect security of SSA-provided information (e.g. implementation of new data access method), or

3) a reported PII breach within the state.

B. Low Risk Criteria

1) no prior review finding(s) or prior finding(s) documented as closed

2) no implementation of technical/operational controls that impact security of SSA provided

3) information (e.g. implementation of new data access method) no reported PII breach

6.5.1 EIEP Compliance Review Participation

SSA may request to meet with the following stakeholders during the compliance review:

a) a sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action

b) the individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement

c) a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information

d) the individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement

e) any additional individuals as deemed appropriate by SSA (i.e. analysts, Project/Program Manager, claims reps, etc.)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

6.6 Scheduling the Onsite Review

SSA will not schedule the onsite review until SSA approves the EIEP's SDP or the EIEPs stakeholders participating in the compliance review have agreed upon a schedule. There is no prescribed period for arranging the subsequent onsite review (***certification review*** for an EIEP requesting initial access to SSA-provided information for an initial agreement or ***compliance review*** for other EIEPs). Unless there are compelling circumstances precluding it; the onsite review will occur as soon as reasonably possible.

The scheduling of the onsite review may depend on additional factors including:

a) the reason for submission of an SDP or CRQ,

b) the severity of security issues, if any,

c) circumstances of the previous review, if any, and

d) SSA's workload and resource considerations.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

7. Additional Definitions

Back Button:

Refers to a button on a web browser's toolbar, the *backspace button* on a computer keyboard, a programmed keyboard button or mouse button, etc., that returns a user to a previously visited web page or application screen.

Breach:

Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording

Browsing:

Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

Choke Point:

The firewall between a local network and the Internet is a choke point in network security, because any attacker would have to come through that channel, which is typically protected and monitored.

Cloud Computing:

The term refers to Internet-based computing derived from the cloud drawing representing the Internet in computer network diagrams. Cloud computing providers deliver on-line and on-demand Internet services. Cloud Services normally use a browser or Web Server to deliver and store information.

Cloud Computing (NIST SP 800-145 Excerpt):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

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

Deployment Models:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific

community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

_____

1 Typically this is done on a pay-per-use or charge-per-use basis.

2 A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

3 This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Cloud Drive:

A cloud drive is a Web-based service that provides storage space on a remote server.

Cloud Audit:

Cloud Audit is a specification developed at Cisco Systems, Inc. that provides cloud computing service providers a standard way to present and share detailed, automated statistics about performance and security.

The Federal Risk and Authorization Program (FedRAMP):
FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

Commingling:

Commingling is the creation of a common database or repository that stores and maintains both SSA-provided information and preexisting EIEP PII.

Data Exchange:

Data Exchange is a logical transfer of information from one government entity's systems of records (SOR) to another agency's application or mainframe through a secure and exclusive connection.

Degaussing:

Degaussing is the method of using a "special device" (i.e., a device that generates a magnetic field) in order to disrupt magnetically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).

Function:

One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. The purpose, activity, or role assigned to one or more persons or organizational components.

Hub:

As it relates to electronic data exchange with SSA, a hub is an organization, which serves as an electronic information conduit or distribution collection point. The term Hub is interchangeable with the terms "StateTransmission Component," "State Transfer Component," or "STC."

ICON:

Interstate Connection Network (various entities use 'Connectivity' rather than 'Connection')

IV & V:

Independent Verification and Validation

Legacy System:

A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receives support from the original vendors or developers.

Manual Transaction:

A user-initiated operation (also referred to as a "user-initiated transaction"). This is the opposite of a system-generated automated process.

Example: A user enters a client's information including the client's SSN and presses the "ENTER" key to acknowledge that input of data is complete. A new screen appears with multiple options, which include "VERIFY SSN" and "CONTINUE". The user has the option to verify the client's SSN or perform alternative actions.

Media Sanitization:

f) Disposal: Refers to the discarding (e.g., recycling) media that contains no sensitive or confidential data.

g) Overwriting/Clearing: This type of media sanitization is adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing.

This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization is not possible on un-writeable or damaged media.

h) Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms *clearing* and *purging* are sometimes synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most re-writeable media requires a single overwrite, purging may require multiple rewrites using different characters for each write cycle.

This is because a laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

i) Degaussing is also an example of an acceptable method for purging magnetic media. The EIEP should destroy media if purging is not a viable method for sanitization.

- Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.

Permission module:

A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN. A properly configured Permission Module also enforces referential integrity and prevents unauthorized random browsing of PII.

Screen Scraping:

Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

Security Breach:

An act from outside an organization that bypasses or violates security policies, practices, or procedures.

Security Incident:

A security incident happens when a fact or event signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats**.**

Security Violation:

An act from within an organization that bypasses or disobeys security policies, practices, or procedures.

Sensitive data:

Sensitive data is a special category of personally identifiable information (PII) that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. It is sensitive information protected against unwarranted disclosure and carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse. Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

Security Information Management (SIM):

SIM is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. The SIM translates the data into correlated and simplified formats.

SMDS (Switched Multimegabit Data Service (SMDS):

SMDS is a telecommunications service that provides connectionless, high-performance, packet- switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.

SSA-provided data/information:

Synonymous with "SSA-supplied data/information", defines information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of SSA-provided data/information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

SSA data/information:

This term, sometimes used interchangeably with "SSA-provided data/information," denotes information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. However, **"SSA data/information"** also includes information provided to the EIEP by a source other than SSA, but which the EIEP attests to that SSA verified it, or the EIEP couples the information with data from SSA as to to certify the accuracy of the information. The following are examples of SSA information:

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN

- Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided by SSA
- Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided to the EIEP by a source other than SSA
- Electronic records that contain only SSA's response to a query for verification of an SSN ***and*** the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSN:

Social Security Number

STC:

A State Transmission/Transfer Component is an organization, which performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub).

System-generated transaction:

A transaction automatically triggered by an automated system process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the "ENTER" key to acknowledge that input of data is complete. An automated process then matches the SSN against the organization's database and when the systems finds no match, automatically sends an electronic request for verification of the SSN to SSA.

Systems process:

Systems Process refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:

Third Party pertains to an entity (person or organization) provided access to SSA-provided information by an EIEP or other SSA business partner for which one or more of the following apply:

- is not stipulated access to SSA-provided information by an information-sharing agreement between an EIEP and SSA
- has no data exchange agreement with SSA
- SSA does not directly authorize access to SSA-provided information

Transaction-driven:

This term pertains to an automatically initiated online query of or request for SSA information by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur the automated process meets prescribed conditions.

Uncontrolled transaction:

This term pertains to a transaction that falls outside a permission module. An uncontrolled transaction is not subject to a systematically enforced relationship between an authorized process or application and an existing client record.

8. Regulatory References

- Federal Information Processing Standards (FIPS) Publications
- Federal Information Security Management Act of 2002 (FISMA)
- Homeland Security Presidential Directive (HSPD-12)
- National Institute of Standards and Technology (NIST) Special Publications
- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Management of Federal Information Resources*
- Office of Management and Budget (OMB) Memo M-06-16, *Protection of Sensitive Agency Information, June 23, 2006*
- Office of Management and Budget (OMB) Memo M-07-16, *Memorandum for the Heads of Executive Departments and Agencies May 22, 2007*
- Office of Management and Budget (OMB) Memo M-07-17, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*
- Privacy Act of 1974, as amended

9. Frequently Asked Questions (Click links for answers or additional information)

1. Q: What is a breach of data?
   A: Refer to Security Breach, Security Incident, and Security Violation.

2. Q: What is employee browsing?
   A: Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

3. Q: Okay, so the EIEP submitted the SDP. Can SSA schedule the Onsite

Review?
A: Refer to Scheduling the Onsite Review.

4. Q: What is a **"Permission Module**?"
A: A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. For example, if requests for verification of an SSN for issuance of a driver's license happens automatically from within a state driver's license application. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN.

5. Q: What **"Screen Scraping**?"
A: Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

6. Q: When does an EIEP have to submit an SDP?
A: Refer to When the SDP is Required.

7. Q: Does an EIEP have to submit an SDP when the agreement is renewed?
A: The EIEP does not have to submit an SDP ***because*** the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an EIEP to submit an SDP.
Refer to When the SDP is Required.

8. Q: Is it acceptable to save SSA-provided information with a verified indicator on a (EIEP) workstation if the EIEP uses an encrypted hard drive? If not, what options does the agency have?
A: There is no problem with an EIEP saving SSA-provided information on the encrypted hard drives of computers used to process SSA-provided information if the EIEP retains the information only as provided for in

the EIEP's data-sharing agreement with SSA.
Refer to Data and Communications Security.

9. Q: Does SSA allow EIEPs to use caching of SSA-provided information on the EIEP's workstations?
A: Caching during processing is not a problem. However, SSA-provided information must clear from the cache when the user exits the application. Refer to Data and Communications Security.

10. Q: What does the term "interconnections to other systems" mean?
A: As used in SSA's system security requirements document, the term "interconnections" is the same as the term "connections."

11. Q: Is it acceptable to submit the SDP as a .PDF file?
A: No, it is not. The document must remain editable.

12. Q: Should the EIEP write the SDP from the standpoint of the EIEP SVES (or applicable data element) access itself, or from the standpoint of access to all data provided to the EIEP by SSA?
A: The SDP is to encompass the EIEP's entire electronic access to SSA-provided information as per the electronic data exchange agreement between the EIEP and SSA.
Refer to Developing the SDP.

13. Q: If the EIEP has a "transaction-driven" system, does the EIEP still need a permission module? If employees cannot initiate a query to SSA, why would the EIEP need the permission module?
A: "Transaction driven" means that queries submit requests automatically (and it might depend on the transaction). Depending on the system's design, queries might not be automatic or it may still permit manual transactions. A system may require manual transactions to correct an error. SSA does not prohibit manual transactions if an ATS properly tracks such transactions. If a "transaction-driven" system permits any type of alternate access, it still requires a permission module, even if it restricts users from performing manual transactions. If the system does ***not*** require the user to be in a particular application and/or the query to be for an existing record in the EIEP's system ***before*** the system will allow a query to go through to SSA, it would still need a permission module.

14. Q: What is an Onsite Compliance Review?
A: The Onsite Compliance Review is SSA's periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's management, operational, and technical security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures.
Refer to the Compliance Review Program and Process.

15. Q: What are the criteria for performing an Onsite Compliance Review?
A: The following are criteria for performing the Onsite Compliance Review:

- EIEP initiating new access or new access method for obtaining information from SSA
- EIEP's cyclical review (previous review was performed remotely)
- EIEP has made significant change(s) in its operating or security platform involving SSA-provided information
- EIEP experienced a breach of SSA-provided personally identifying information (PII)
- EIEP has been determined to be high-risk

16. Q: What is a Remote Compliance Review?
A: The Remote Compliance Review is when SSA conducts the meetings remotely (e.g., via conference calls). SSA schedules conference calls with its EIEPs to determine whether the EIEPs technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA"s associated system security requirements and procedures. Refer to the Compliance Review Program and Process.

17. Q: What are the criteria for performing a Remote Compliance Review?
A: The EIEP must satisfy the following criteria to qualify for a Remote Compliance Review:

- EIEP's cyclical review (SSA's previous review yielded no findings or the EIEP satisfactorily resolved cited findings)
- EIEP has made no significant change(s) in its operating or security platform involving SSA-provided information
- EIEP has not experienced a breach of SSA-provided personally identifying information (PII) since its previous compliance review.
- SSA rates the EIEP as a low-risk agency or state

ATTACHMENT 5

SYSTEM CERTIFICATION REQUIREMENTS FOR THE CMS HUB

Not Applicable

Security Certification Requirements for use of the *SSA Data Set* via the Centers for Medicare & Medicaid Services' (CMS) Hub

The Social Security Administration (SSA) does not allow new data exchange partners to begin receiving data electronically until the Authorized State Agency submits an approved Security Design Plan (SDP). SSA's Office of Information Security (OIS) usually performs an onsite security review to verify and validate that the management, operational, and technical controls conform to the requirements of the signed agreements between SSA and the Authorized State Agency, as well as applicable Federal law and SSA's technical systems security requirements (Attachment 4 to the Information Exchange Agreement (IEA)). As it concerns the use of the *SSA Data Set* via the Hub, OIS will waive the initial SDP/Certification for an existing Authorized State Agency if it meets all the following criteria:

1. The Authorized State Agency already has a functioning CMS-approved Integrated Eligibility Verification System (IEVS).
2. The Authorized State Agency is already receiving data from the Hub to support the Medicaid program and/or the Children's Health Insurance Program (CHIP).
3. The Authorized State Agency will only process requests for the *SSA Data Set* for administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency agrees that the SSA security controls identified in the IEA and Attachment 4 to the IEA will prevail for all SSA data received by the State Agency, including the *SSA Data Set*.
5. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through the Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.
6. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.

In the event that an Authorized State Agency decides to implement a new integrated eligibility system or use a different Authorized State Agency to implement the health or income maintenance data exchange process through the Hub, the Authorized State Agency will submit to SSA's OIS an SDP and be approved/certified prior to receipt of the *SSA Data Set* through the Hub. The Authorized State Agency will adhere to the following criteria, in addition to those stated in the IEA, section C, Program Questionnaire:

1. The Authorized State Agency agrees to provide an attestation to SSA that it has received certification through the CMS Hub approval MARS-E process.
2. The Authorized State Agency attests that it operates and has a CMS-approved IEVS and the IEVS initiates the request for the *SSA Data Set* for the State Agency's administration of health or income maintenance programs approved by SSA through the Hub in conjunction with Insurance Affordability Programs eligibility determinations.

3. The Authorized State Agency uses a streamlined multi-benefit application. The Authorized State Agency agrees not to process verification requests through the Hub from a standalone application for health or income maintenance program requests that have no connection to Insurance Affordability Programs eligibility determinations.
4. The Authorized State Agency will not request the *SSA Data Set* through the Hub until it has successfully begun using the Hub for administration of Insurance Affordability Programs eligibility determinations. SSA will begin sending the *SSA Data Set* to the Authorized State Agency after the State Agency verifies that the Hub process works, as required by the CMS Hub approval MARS-E process.
5. The Authorized State Agency agrees to participate in SSA's SDP/Certification process prior to transmitting requests for the *SSA Data Set* through the Hub and to participate in SSA's triennial security compliance reviews on an ongoing basis.
6. The Authorized State Agency agrees that a significant vulnerability or risk in a security control, a data loss, or a security breach may result in a suspension or termination of the *SSA Data Set* through Hub. In this case, at SSA's request, the Authorized State Agency agrees to immediately cease using the *SSA Data Set* for all SSA authorized health or income maintenance programs until the State Agency sufficiently mitigates or eliminates such risk(s) and/or vulnerabilities to SSA's data.

ATTACHMENT 6

WORKSHEET FOR REPORTING LOSS OR PORTENTIAL LOSS

OF PERSONALLY INDETIFIABLE INFORMATION

09/27/06

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information

1. Information about the individual making the report to the NCSC:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (circle one):

If Electronic, what type of device?

Laptop		Tablet		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Blackberry Phone #	
Hard Drive		Floppy Disk		USB Drive			
Other (describe):							

09/27/06

Additional Questions if Electronic:

	Yes	No	Not Sure
a. Was the device encrypted?			
b. Was the device password protected?			
c. If a laptop or tablet, was a VPN SmartCard lost?			
Cardholder's Name:			
Cardholder's SSA logon PIN:			
Hardware Make/Model:			
Hardware Serial Number:			

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. **If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:**

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
E-mail Address:					

5. **Circumstances of the loss:**
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. **Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)**

09/27/06

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Other (describe)		

8. Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):