CALIFORNIA
LOW INCOME HOME ENERGY ASSISTANCE PROGRAM
DRAFT STATE PLAN

LOW **I**NCOME **H**OME **E**NERGY **A**SSISTANCE **P**ROGRAM
Federal Fiscal Year 2021

Gavin Newsom
GOVERNOR

State of California
Mark Ghaly
SECRETARY
Health and Human Services Agency

David Scribner
ACTING DIRECTOR

Department of Community Services and Development
U.S. Department of Health and Human Services
Administration for Children and Families
Office of Community Services

DETAILED MODEL PLAN (LIHEAP)

Program Name: Low Income Home Energy Assistance
Grantee Name: California
Report Name: DETAILED MODEL PLAN (LIHEAP)
Report Period: 10/01/2020 to 09/30/2021
Report Status: Saved

Report Sections

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

* 1.a. Type of Submission:	* 1.b. Frequency:	* 1.c. Consolidated Application/ Plan/Funding Request? Explanation:	* 1.d. Version:
(•) Plan	(•) Annual		(•) Initial ( ) Resubmission ( ) Revision ( ) Update
		2. Date Received:	State Use Only:
		3. Applicant Identifier:	
		4a. Federal Entity Identifier:	5. Date Received By State:
		4b. Federal Award Identifier:	6. State Application Identifier:

7. APPLICANT INFORMATION

*** a. Legal Name:** State of California

* b. Employer/Taxpayer Identification Number (EIN/TIN):	* c. Organizational DUNS:
68-0283471	929578268

*** d. Address:**

* Street 1:	2389 GATEWAY OAKS DR., STE. 100	Street 2:	
* City:	SACRAMENTO	County:	
* State:	CA	Province:	
* Country:	United States	* Zip / Postal Code:	95833-4246

e. Organizational Unit:

Department Name:	Division Name:
Department of Community Services and Development	Energy and Environmental Services

f. Name and contact information of person to be contacted on matters involving this application:

Prefix:	* First Name:	Middle Name:	* Last Name:
	Kathy		Andry
Suffix:	**Title:** LIHEAP Director	**Organizational Affiliation:** N/A	
*** Telephone Number:** 916-576-7154	**Fax Number** 916-263-1406	*** Email:** kathy.andry@csd.ca.gov	

*** 8a. TYPE OF APPLICANT:**
A: State Government

b. Additional Description:

*** 9. Name of Federal Agency:**

	Catalog of Federal Domestic Assistance Number:	CFDA Title:
10. CFDA Numbers and Titles	93568	Low-Income Home Energy Assistance

11. Descriptive Title of Applicant's Project
LIHEAP provides assistance to eligible low-income households to manage and meet their immediate home heating and/or cooling needs.

12. Areas Affected by Funding:
State of California

13. CONGRESSIONAL DISTRICTS OF:			
* a. Applicant 5		b. Program/Project: CA	
Attach an additional list of Program/Project Congressional Districts if needed.			
14. FUNDING PERIOD:		15. ESTIMATED FUNDING:	
a. Start Date: 10/01/2020	b. End Date: 09/30/2021	* a. Federal ($): $0	b. Match ($): $0

*** 16. IS SUBMISSION SUBJECT TO REVIEW BY STATE UNDER EXECUTIVE ORDER 12372 PROCESS?**

a. This submission was made available to the State under the Executive Order 12372

Process for Review on :

b. Program is subject to E.O. 12372 but has not been selected by State for review.

c. Program is not covered by E.O. 12372.

*** 17. Is The Applicant Delinquent On Any Federal Debt?**

○ YES

◉ NO

Explanation:

18. By signing this application, I certify (1) to the statements contained in the list of certifications and (2) that the statements herein are true, complete and accurate to the best of my knowledge. I also provide the required assurances** and agree to comply with any resulting terms if I accept an award. I am aware that any false, fictitious, or fraudulent statements or claims may subject me to criminal, civil, or administrative penalties. (U.S. Code, Title 218, Section 1001)**

****I Agree** ☑

**** The list of certifications and assurances, or an internet site where you may obtain this list, is contained in the announcement or agency specific instructions.**

18a. Typed or Printed Name and Title of Authorized Certifying Official	18c. Telephone (area code, number and extension)
	18d. Email Address
18b. Signature of Authorized Certifying Official	18e. Date Report Submitted (Month, Day, Year)

Attach supporting documents as specified in agency instructions.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Department of Health and Human Services
Administration for Children and Families
Office of Community Services
Washington, DC 20201

August 1987, revised 05/92, 02/95, 03/96, 12/98, 11/01
OMB Approval No. 0970-0075
Expiration Date: 09/30/2020

THE PAPERWORK REDUCTION ACT OF 1995 (Pub. L. 104-13)Use of this model plan is optional. However, the information requested is required in order to receive a Low Income Home Energy Assistance Program (LIHEAP) grant in years in which the grantee is not permitted to file an abbreviated plan. Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, gathering and maintaining the data needed, and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

Section 1 Program Components

Program Components, 2605(a), 2605(b)(1) - Assurance 1, 2605(c)(1)(C)

1.1 Check which components you will operate under the LIHEAP program. (Note: You must provide information for each component designated here as requested elsewhere in this plan.)		Dates of Operation	
		Start Date	End Date
☑	Heating assistance	10/01/2020	09/30/2021
☑	Cooling assistance	10/01/2020	09/30/2021
☑	Crisis assistance	10/01/2020	09/30/2021
☑	Weatherization assistance	10/01/2020	09/30/2021

Provide further explanation for the dates of operation, if necessary

The 2020 Contract Term runs from 10/01/2020 through 06/30/2022. The intent of the contract term is to ensure continuation of services in the event that federal funds are not released by 10/01/2020. Local Service Providers are expected to expend funds by November 2021.

Estimated Funding Allocation, 2604(C), 2605(k)(1), 2605(b)(9), 2605(b)(16) - Assurances 9 and 16

1.2 Estimate what amount of available LIHEAP funds will be used for each component that you will operate: The total of all percentages must add up to 100%.	Percentage (%)
Heating assistance	21.00%
Cooling assistance	6.00%
Crisis assistance	33.00%
Weatherization assistance	15.00%
Carryover to the following federal fiscal year	10.00%

Administrative and planning costs	10.00%
Services to reduce home energy needs including needs assessment (Assurance 16)	5.00%
Used to develop and implement leveraging activities	0.00%
TOTAL	100.00%

Alternate Use of Crisis Assistance Funds, 2605(c)(1)(C)

1.3 The funds reserved for winter crisis assistance that have not been expended by March 15 will be reprogrammed to:

☑	Heating assistance	☑	Cooling assistance
☑	Weatherization assistance	☑	Other (specify:) CSD provides crisis assistance throughout the program year.

Categorical Eligibility, 2605(b)(2)(A) - Assurance 2, 2605(c)(1)(A), 2605(b)(8A) - Assurance 8

1.4 Do you consider households categorically eligible if one household member receives one of the following categories of benefits in the left column below? ○ Yes ◉ No

If you answered "Yes" to question 1.4, you must complete the table below and answer questions 1.5 and 1.6.

	Heating	Cooling	Crisis	Weatherization
TANF	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
SSI	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
SNAP	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No
Means-tested Veterans Programs	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No

	Program Name	Heating	Cooling	Crisis	Weatherization
Other(Specify) 1		○ Yes ○ No	○ Yes ○ No	○ Yes ○ No	○ Yes ○ No

1.5 Do you automatically enroll households without a direct annual application? ○ Yes ◉ No

If Yes, explain:

1.6 How do you ensure there is no difference in the treatment of categorically eligible households from those not receiving other public assistance when determining eligibility and benefit amounts?

SNAP Nominal Payments

1.7a Do you allocate LIHEAP funds toward a nominal payment for SNAP households? ○ Yes ◉ No

If you answered "Yes" to question 1.7a, you must provide a response to questions 1.7b, 1.7c, and 1.7d.

1.7b Amount of Nominal Assistance: $0.00

1.7c Frequency of Assistance

☐	Once Per Year
☐	Once every five years
☐	Other - Describe:

1.7d How do you confirm that the household receiving a nominal payment has an energy cost or need?

Determination of Eligibility - Countable Income

1.8. In determining a household's income eligibility for LIHEAP, do you use gross income or net income ?

☑	Gross Income
☐	Net Income

1.9. Select all the applicable forms of countable income used to determine a household's income eligibility for LIHEAP

☑	Wages

☑	**Self - Employment Income**
☐	**Contract Income**
☐	**Payments from mortgage or Sales Contracts**
☑	**Unemployment insurance**
☑	**Strike Pay**
☑	**Social Security Administration (SSA) benefits**
	☐ **Including MediCare deduction** ☑ **Excluding MediCare deduction**
☑	**Supplemental Security Income (SSI)**
☑	**Retirement / pension benefits**
☑	**General Assistance benefits**
☑	**Temporary Assistance for Needy Families (TANF) benefits**
☐	**Supplemental Nutrition Assistance Program (SNAP) benefits**
☐	**Women, Infants, and Children Supplemental Nutrition Program (WIC) benefits**
☐	**Loans that need to be repaid**
☐	**Cash gifts**
☐	**Savings account balance**
☐	**One-time lump-sum payments, such as rebates/credits, winnings from lotteries, refund deposits, etc.**
☑	**Jury duty compensation**
☑	**Rental income**
☐	**Income from employment through Workforce Investment Act (WIA)**
☐	**Income from work study programs**
☑	**Alimony**
☑	**Child support**
☑	**Interest, dividends, or royalties**
☑	**Commissions**
☐	**Legal settlements**
☑	**Insurance payments made directly to the insured**
☐	**Insurance payments made specifically for the repayment of a bill, debt, or estimate**

☑	**Veterans Administration (VA) benefits**
☐	**Earned income of a child under the age of 18**
☐	**Balance of retirement, pension, or annuity accounts where funds cannot be withdrawn without a penalty.**
☐	**Income tax refunds**
☐	**Stipends from senior companion programs, such as VISTA**
☐	**Funds received by household for the care of a foster child**
☐	**Ameri-Corp Program payments for living allowances, earnings, and in-kind aid**
☐	**Reimbursements (for mileage, gas, lodging, meals, etc.)**
☐	**Other**

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 2 - Heating Assistance

Eligibility, 2605(b)(2) - Assurance 2

2.1 Designate the income eligibility threshold used for the heating component:

Add	Household size	Eligibility Guideline	Eligibility Threshold
1	All Household Sizes	State Median Income	60.00%

2.2 Do you have additional eligibility requirements for HEATING ASSITANCE?	○ Yes ◉ No
2.3 Check the appropriate boxes below and describe the policies for each.	
Do you require an Assets test ?	○ Yes ◉ No
Do you have additional/differing eligibility policies for:	
Renters?	○ Yes ◉ No
Renters Living in subsidized housing ?	○ Yes ◉ No
Renters with utilities included in the rent ?	○ Yes ◉ No
Do you give priority in eligibility to:	
Elderly?	◉ Yes ○ No
Disabled?	◉ Yes ○ No
Young children?	◉ Yes ○ No
Households with high energy burdens ?	◉ Yes ○ No
Other?	○ Yes ◉ No

Explanations of policies for each "yes" checked above:

Based on an assesment of each client, Local Service Providers assign points and priority may be given to households with life-threatening emergencies.

Additional points are provided to households that include persons 60 years or older, persons 5 years or younger, and disabled persons.

Determination of Benefits 2605(b)(5) - Assurance 5, 2605(c)(1)(B)

2.4 Describe how you prioritize the provision of heating assistance tovulnerable populations,e.g., benefit amounts, early application periods, etc.

Based on an assessment of each client, Local Service Providers assign points and priority may be given to households with life-threatening emergencies.

Additional points are provided to households that include persons 60 years or older, persons 5 years or younger, and disabled persons.

2.5 Check the variables you use to determine your benefit levels. (Check all that apply):

- ☑ **Income**
- ☑ **Family (household) size**
- ☑ **Home energy cost or need:**

☐ **Fuel type**	
☐ **Climate/region**	
☐ **Individual bill**	
☐ **Dwelling type**	
☐ **Energy burden (% of income spent on home energy)**	
☑ **Energy need**	
☑ **Other - Describe:**	

CSD conducts an "Individual Utility Company Rate Survey" each year. In the survey, utility companies report their residential rates, by county, for gas and electricity. CSD uses this information to establish average utility costs for each county. These costs are factored into the heating and cooling benefit formula to determine LIHEAP benefit levels.

Benefit Levels, 2605(b)(5) - Assurance 5, 2605(c)(1)(B)

2.6 Describe estimated benefit levels for FY 2020:

Minimum Benefit	$144	**Maximum Benefit**	$1,000

2.7 Do you provide in-kind (e.g., blankets, space heaters) and/or other forms of benefits? ○ Yes ◉ No

If yes, describe.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 3 - Cooling Assistance

Eligibility, 2605(c)(1)(A), 2605 (b)(2) - Assurance 2

3.1 Designate The income eligibility threshold used for the Cooling component:

Add	Household size	Eligibility Guideline	Eligibility Threshold
1	All Household Sizes	State Median Income	60.00%

3.2 Do you have additional eligibility requirements for COOLING ASSITANCE?	○ Yes ◉ No
3.3 Check the appropriate boxes below and describe the policies for each.	
Do you require an Assets test ?	○ Yes ◉ No
Do you have additional/differing eligibility policies for:	
Renters?	○ Yes ◉ No
Renters Living in subsidized housing ?	○ Yes ◉ No
Renters with utilities included in the rent ?	○ Yes ◉ No
Do you give priority in eligibility to:	
Elderly?	◉ Yes ○ No
Disabled?	◉ Yes ○ No
Young children?	◉ Yes ○ No
Households with high energy burdens ?	◉ Yes ○ No
Other?	○ Yes ◉ No

Explanations of policies for each "yes" checked above:

3.4 Describe how you prioritize the provision of cooling assistance tovulnerable populations,e.g., benefit amounts, early application periods, etc.

Based on an assessment of each client, Local Service Providers assign points and priority may be given to households with life-threatening emergencies.

Determination of Benefits 2605(b)(5) - Assurance 5, 2605(c)(1)(B)

3.5 Check the variables you use to determine your benefit levels. (Check all that apply):

- ☑ **Income**
- ☑ **Family (household) size**
- ☑ **Home energy cost or need:**
  - ☐ **Fuel type**
  - ☐ **Climate/region**
  - ☐ **Individual bill**
  - ☐ **Dwelling type**

☐ Energy burden (% of income spent on home energy)	
☑ Energy need	
☑ Other - Describe:	

CSD conducts an "Individual Utility Company Rate Survey" each year. In the survey, utility companies report their residential rates, by county, for gas and electricity. CSD uses this information to establish average utility costs for each county. These costs are factored into the heating and cooling benefit formula to determine LIHEAP benefit levels.

Benefit Levels, 2605(b)(5) - Assurance 5, 2605(c)(1)(B)

3.6 Describe estimated benefit levels for FY 2020:

Minimum Benefit	$144	**Maximum Benefit**	$1,000

3.7 Do you provide in-kind (e.g., fans, air conditioners) and/or other forms of benefits? ○ Yes ◉ No

I f y s,desc rb e

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 4: CRISIS ASSISTANCE

Eligibility - 2604(c), 2605(c)(1)(A)

4.1 Designate the income eligibility threshold used for the crisis component

Add	Household size	Eligibility Guideline	Eligibility Threshold
1	All Household Sizes	State Median Income	60.00%

4.2 Provide your LIHEAP program's definition for determining a crisis.

CSD uses the federal definition of a crisis (Low Income Energy Assistance Act § 2603 (3)): "weather-related and supply shortage emergencies and other household energy related emergencies." Crisis funds may only be used in accordance with the federal definition, including:

1. A natural disaster (whether or not officially declared),
2. A significant home energy supply shortage or disruption,
3. An official declaration of a significant increase in:
4. - Home energy costs,
5. - Home energy disconnections,
6. - Enrollment in public benefit programs, or
7. - Unemployment and layoffs, or
8. An official emergency declaration by the Secretary of Health and Human Services,

In those situations where there is not an official federal, state, or local declaration of emergency, an emergency may be deemed to exist by CSD where there is imminent danger, requiring immediate action to prevent or mitigate the loss or impairment of life, health, property, or essential public services.

4.3 What constitutes a life-threatening crisis?

Life-Threatening: Applicant is without heating, cooling or utility service during extreme weather conditions, as determined by the local administrative agency. This may include energy-related situations that pose a threat to the heath and safety of one or more members of the household.

Crisis Requirement, 2604(c)

4.4 Within how many hours do you provide an intervention that will resolve the energy crisis for eligible households? 48**Hours**

4.5 Within how many hours do you provide an intervention that will resolve the energy crisis for eligible households in life-threatening situations? 18**Hours**

Crisis Eligibility, 2605(c)(1)(A)

4.6 Do you have additional eligibility requirements for CRISIS ASSISTANCE?	(•) Yes ( ) No
4.7 Check the appropriate boxes below and describe the policies for each	
Do you require an Assets test ?	( ) Yes (•) No
Do you give priority in eligibility to :	
Elderly?	(•) Yes ( ) No
Disabled?	(•) Yes ( ) No
Young Children?	(•) Yes ( ) No
Households with high energy burdens?	(•) Yes ( ) No

Other? See explanation below	(•) Yes ( ) No
In Order to receive crisis assistance:	
Must the household have received a shut-off notice or have a near empty tank?	(•) Yes ( ) No
Must the household have been shut off or have an empty tank?	( ) Yes (•) No
Must the household have exhausted their regular heating benefit?	( ) Yes (•) No
Must renters with heating costs included in their rent have received an eviction notice ?	( ) Yes (•) No
Must heating/cooling be medically necessary?	( ) Yes (•) No
Must the household have non-working heating or cooling equipment?	( ) Yes (•) No
Other? Proof of utility shutoff notice, Proof of energy termination, Insufficient funds to establish a new energy account, Insufficient funds to pay a delinquent utility bill, Insufficient funds to pay for essential firewood, oil or propane, Insufficient funds to pay the cost of repairing or replacing an eligible heating or cooling appliance or for a new heating or cooling appliance, and/or Applicant has a medical condition that requires temperature or climate control and the heating/cooling appliance is considered hazardous, nonexistent, or inoperable	(•) Yes ( ) No
Do you have additional / differing eligibility policies for:	
Renters?	( ) Yes (•) No
Renters living in subsidized housing?	( ) Yes (•) No
Renters with utilities included in the rent?	( ) Yes (•) No
Explanations of policies for each "yes" checked above:	

Each Local Service Provider is required to submit a priority plan as an attachment to their contract. The priority plans are in narrative format and identify multiple categories used to prioritize services, such as: Poverty Level, Energy Burden, Vulnerable Population. Based on an assessment of each applicant, Local Service Providers prioritize by assigning points for each of these categories though priority may be given to households with life-threatening emergencies.

Determination of Benefits

4.8 How do you handle crisis situations?

☑	**Separate component**
☑	**Fast Track**
☑	**Other - Describe:**

The Crisis Program is limited to five activities:

1. Fast Track (electric and gas) utility payments
2. Energy Crisis Intervention Program Wood, propane and oil (ECIP WPO) payments
3. Heating and cooling services (HCS)
4. Severe Weather Energy Assistance and Transportation Services (SWEATS)
5. Public Safety Power Shutoff (PSPS) Pilot Program

Fast Track benefits are determined by the Local Service Providers, but payments to the utility companies are processed, centrally, by CSD, where ECIP WPO assistance, HCS and SWEATS benefits are provided locally. Local Service Providers have the ability to increase the Fast Track base amount by adding a supplemental benefit. The total benefit amount cannot exceed the total amount of the entire utility bills (to include energy charges, reconnection fees, and other assessed utility fees/surcharges to alleviate the crisis situation) or $1,000, whichever is less.

ECIP WPO benefits are determined at the local level based on clients inability to pay for essential firewood, oil or propane. The amount of the benefit is based on the cost to resolve the crisis.

HCS services provide payment for energy-related repairs or replacement of non-functioning heating, cooling appliances and water-heating appliances. The benefit amount is based on the cost of the repair or replacement, up to the maximum amount as determined annually.

SWEATS services provide payment to address energy-related emergency needs of low-income households affected by a natural disaster and PSPS. Typical services include additional utility assistance, temporary housing services, transportation services, temporary heating/cooling devices, and battery backup devices. The amount of the benefit may vary depending on the benefit offered.

PSPS Emergency Preparedness Pilot services low-income households medically vulnerable to the effects of energy-related emergencies and residing in designated High Fire Risk Areas. As a pilot, it is designed to collect detailed reporting in order to further develop the PSPS Emergency Preparedness component and to aid LSPs in leveraging other

	resources to implement Emergency Preparedness services. Services include household emergency risk assessment, PSPS preparedness education, emergency preparedness supplies, and backup power appliances.

4.9 If you have a separate component, how do you determine crisis assistance benefits?

☑	**Amount to resolve the crisis.**
☑	**Other - Describe:** *Fast Track* benefits are determined by the Local Service Providers, but payments to the utility companies are processed, centrally, by CSD, where ECIP WPO assistance, HCS and SWEATS benefits are provided locally. Local Service Providers have the ability to increase the Fast Track base amount by adding a supplemental benefit. The total benefit amount cannot exceed the total amount of the entire utility bills (to include energy charges, reconnection fees, and other assessed utility fees/surcharges to alleviate the crisis situation) or $1,000, whichever is less.

Crisis Requirements, 2604(c)

4.10 Do you accept applications for energy crisis assistance at sites that are geographically accessible to all households in the area to be served?

◉ Yes ○ No **Explain.**

Large service territories typically have satellite offices or other non-profit agencies which accept applications.

4.11 Do you provide individuals who are physically disabled the means to:

Submit applications for crisis benefits without leaving their homes?

◉ Yes ○ No **If No, explain.**

Travel to the sites at which applications for crisis assistance are accepted?

◉ Yes ○ No **If No, explain.**

If you answered "No" to both options in question 4.11, please explain alternative means of intake to those who are homebound or physically disabled?

Benefit Levels, 2605(c)(1)(B)

4.12 Indicate the maximum benefit for each type of crisis assistance offered.

Winter Crisis	$0.00 **maximum benefit**
Summer Crisis	$0.00 **maximum benefit**
Year-round Crisis	$1,000.00 **maximum benefit**

4.13 Do you provide in-kind (e.g. blankets, space heaters, fans) and/or other forms of benefits?

◉ Yes ○ No **If yes, Describe**

Space heaters are allowable under the Emergency Heating and Cooling Program (EHCS). Evaporative coolers, heaters, fans, battery power backup devices, and generators are allowable under the Severe Weather Energy Assistance and Transportation Program (SWEATS).

4.14 Do you provide for equipment repair or replacement using crisis funds?

◉ Yes ○ No

If you answered "Yes" to question 4.14, you must complete question 4.15.

4.15 Check appropriate boxes below to indicate type(s) of assistance provided.

	Winter Crisis	Summer Crisis	Year-round Crisis
Heating system repair	☐	☐	☑
Heating system replacement	☐	☐	☑
Cooling system repair	☐	☐	☑
Cooling system replacement	☐	☐	☑
Wood stove purchase	☐	☐	☑
Pellet stove purchase	☐	☐	☑

Solar panel(s)	☐	☐	☐
Utility poles / gas line hook-ups	☐	☐	☐
Other (Specify): Water Heater	☐	☐	☑

4.16 Do any of the utility vendors you work with enforce a moratorium on shut offs?

○ Yes ◉ No

If you responded "Yes" to question 4.16, you must respond to question 4.17.

4.17 Describe the terms of the moratorium and any special dispensation received by LIHEAP clients during or after the moratorium period.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 5: WEATHERIZATION ASSISTANCE

Eligibility, 2605(c)(1)(A), 2605(b)(2) - Assurance 2

5.1 Designate the income eligibility threshold used for the Weatherization component

Add	Household Size	Eligibility Guideline	Eligibility Threshold
1	All Household Sizes	State Median Income	60.00%

5.2 Do you enter into an interagency agreement to have another government agency administer a WEATHERIZATION component? ○ Yes ◉ No

5.3 If yes, name the agency.

5.4 Is there a separate monitoring protocol for weatherization? ◉ Yes ○ No

WEATHERIZATION - Types of Rules

5.5 Under what rules do you administer LIHEAP weatherization? (Check only one.)

- ☐ **Entirely under LIHEAP (not DOE) rules**
- ☐ **Entirely under DOE WAP (not LIHEAP) rules**
- ☑ **Mostly under LIHEAP rules with the following DOE WAP rule(s) where LIHEAP and WAP rules differ (Check all that apply):**
  - ☐ **Income Threshold**
  - ☑ **Weatherization of entire multi-family housing structure is permitted if at least 66% of units (50% in 2- & 4-unit buildings) are eligible units or will become eligible within 180 days**
  - ☐ **Weatherize shelters temporarily housing primarily low income persons (excluding nursing homes, prisons, and similar institutional care facilities).**
  - ☐ **Other - Describe:**
- ☐ **Mostly under DOE WAP rules, with the following LIHEAP rule(s) where LIHEAP and WAP rules differ (Check all that apply.)**
  - ☐ **Income Threshold**
  - ☐ **Weatherization not subject to DOE WAP maximum statewide average cost per dwelling unit.**
  - ☐ **Weatherization measures are not subject to DOE Savings to Investment Ration (SIR) standards.**
  - ☐ **Other - Describe:**

Eligibility, 2605(b)(5) - Assurance 5

5.6 Do you require an assets test?	○ Yes ◉ No
5.7 Do you have additional/differing eligibility policies for :	
Renters	○ Yes ◉ No
Renters living in subsidized housing?	○ Yes ◉ No
5.8 Do you give priority in eligibility to:	
Elderly?	◉ Yes ○ No
Disabled?	◉ Yes ○ No

Young Children?	(•) Yes ( ) No
House holds with high energy burdens?	(•) Yes ( ) No
Other? See explanation below	(•) Yes ( ) No

If you selected "Yes" for any of the options in questions 5.6, 5.7, or 5.8, you must provide further explanation of these policies in the text field below.

CSD will implement the new Priority Plan for 2021 that prioritizes applicants based on income, energy burden, and vulnerable population (elderly, disabled, and families with young children).

Benefit Levels

5.9 Do you have a maximum LIHEAP weatherization benefit/expenditure per household? (•) Yes ( ) No

5.10 If yes, what is the maximum? $7,669

Types of Assistance, 2605(c)(1), (B) & (D)

5.11 What LIHEAP weatherization measures do you provide ? (Check all categories that apply.)

☑ **Weatherization needs assessments/audits**	☑ **Energy related roof repair**
☑ **Caulking and insulation**	☑ **Major appliance Repairs**
☑ **Storm windows**	☑ **Major appliance replacement**
☑ **Furnace/heating system modifications/ repairs**	☑ **Windows/sliding glass doors**
☑ **Furnace replacement**	☑ **Doors**
☑ **Cooling system modifications/ repairs**	☑ **Water Heater**
☑ **Water conservation measures**	☑ **Cooling system replacement**
☑ **Compact florescent light bulbs**	☑ **Other - Describe:** Please see attachment

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 6: Outreach, 2605(b)(3) - Assurance 3, 2605(c)(3)(A)

6.1 Select all outreach activities that you conduct that are designed to assure that eligible households are made aware of all LIHEAP assistance available:

- [x] **Place posters/flyers in local and county social service offices, offices of aging, Social Security offices, VA, etc.**
- [x] **Publish articles in local newspapers or broadcast media announcements.**
- [x] **Include inserts in energy vendor billings to inform individuals of the availability of all types of LIHEAP assistance.**
- [x] **Mass mailing(s) to prior-year LIHEAP recipients.**
- [x] **Inform low income applicants of the availability of all types of LIHEAP assistance at application intake for other low-income programs.**
- [x] **Execute interagency agreements with other low-income program offices to perform outreach to target groups.**
- [x] **Other (specify):**
  - Partnerships with utility companies
  - Outreach to: legislative offices, community organizations, and attendance at community events
  - Referrals to CSD's programs from child care centers
  - Pamphlets
  - Toll-free phone line
  - CSD's website
  - Contractors' websites
  - Special events
  - Canvass neighborhoods and go door to door
  - Distributes flyers at schools

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 7: Coordination, 2605(b)(4) - Assurance 4

7.1 Describe how you will ensure that the LIHEAP program is coordinated with other programs available to low-income households (TANF, SSI, WAP, etc.).

☐	**Joint application for multiple programs**
☑	**Intake referrals to/from other programs**
☑	**One - stop intake centers**
☑	**Other - Describe:**

CSD and Local Service Providers coordinate activities with similar and related programs administered by the federal, state, and the public and private sector, particularly low-income, energy conservation programs. CSD is working with the California Public Utilities Commission (CPUC) and the state's investor owned utility companies to develop strategies to better leverage and coordinate our mutual resources to benefit low-income households in the state.

Local Service Providers refer potentially eligible applicants, including heating and cooling, and crisis applicants, to the weatherization program, California Alternate Rate for Energy (CARE), Reduced Rate Programs (RRP), and/or to other energy or conservation programs. This referral is accomplished through interagency agreements, communications with pertinent agencies, one-stop centers, utility companies, and public/ private partnerships. Local Service Providers provide assistance in coordinating the payment of client's energy/utility bill with the appropriate energy vendor or utility company.

CSD administers a state funded Low-Income Weatherization (LIWP) program that offers weatherization and renewable energy services to low-income households that resides in disadvantage communities as defined in CalEnviroScreen 3.0. CSD is working on policies to prevent duplication.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 8: Agency Designation, 2605(b)(6) - Assurance 6 (Required for state grantees and the Commonwealth of Puerto Rico)

8.1 How would you categorize the primary responsibility of your State agency?

☑	**Administration Agency**
☐	**Commerce Agency**
☐	**Community Services Agency**
☐	**Energy / Environment Agency**
☐	**Housing Agency**
☐	**Welfare Agency**
☐	**Other - Describe:**

Alternate Outreach and Intake, 2605(b)(15) - Assurance 15

If you selected "Welfare Agency" in question 8.1, you must complete questions 8.2, 8.3, and 8.4, as applicable.

8.2 How do you provide alternate outreach and intake for HEATING ASSISTANCE?

N/A

8.3 How do you provide alternate outreach and intake for COOLING ASSISTANCE?

N/A

8.4 How do you provide alternate outreach and intake for CRISIS ASSISTANCE?

N/A

8.5 LIHEAP Component Administration.	Heating	Cooling	Crisis	Weatherization
8.5a Who determines client eligibility?	Community Action Agencies	Community Action Agencies	Community Action Agencies	Community Action Agencies
8.5b Who processes benefit payments to gas and electric vendors?	State Administration Agency	State Administration Agency	State Administration Agency	

8.5c who processes benefit payments to bulk fuel vendors?	Community Action Agencies	Community Action Agencies	Community Action Agencies	
8.5d Who performs installation of weatherization measures?				Community Action Agencies

If any of your LIHEAP components are not centrally-administered by a state agency, you must complete questions 8.6, 8.7, 8.8, and, if applicable, 8.9.

8.6 What is your process for selecting local administering agencies?

LIHEAP Local Service Providers were designated pursuant to California Government Code section 16367.5. The LSP network is comprised of 41 Local Service Providers (LSPs), which include private, non-profit and local government service providers. These LSPs have strong ties to their local communities and have many years of experience providing public assistance programs to the low-income customers in their respective service territory.

8.7 How many local administering agencies do you use? 41

8.8 Have you changed any local administering agencies in the last year?

- ○ Yes
- ◉ No

8.9 If so, why?

- ☐ **Agency was in noncompliance with grantee requirements for LIHEAP -**
- ☐ **Agency is under criminal investigation**
- ☐ **Added agency**
- ☐ **Agency closed**
- ☐ **Other - describe**

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 9: Energy Suppliers, 2605(b)(7) - Assurance 7

9.1 Do you make payments directly to home energy suppliers?

Heating	(•) Yes ( ) No
Cooling	(•) Yes ( ) No
Crisis	(•) Yes ( ) No
Are there exceptions?	(•) Yes ( ) No

If yes, Describe.

In most cases, direct payments are issued to energy vendors. Occasionally, dual party warrants are issued and are made payable to the client and the energy vendor. On those few occasions when utilities are included in the rent or sub-metered, warrants are issued directly to the client.

For those heating and cooling and crisis clients whose energy source is WPO, Local Service Providers make payment directly to energy vendors.

9.2 How do you notify the client of the amount of assistance paid?

1. When a payment is made directly to an energy vendor, the Local Service Provider sends the client a letter, advising them of the LIHEAP payment amount and approximate date the benefit will be credited to the account.

2. When a crisis, and/or heating and cooling payment is made to an applicant with utilities included in rent, submetered utilities or with non-participating utility companies, the Local Service Provider provides the client letter indicating the amount of the benfit and the utility company to be paid, if applicable.

3. When a crisis, and/or heating and cooling payment is made directly to an energy vendor, the vendor shows the amount of credit on the customer's bill, indicating that the payment was made by LIHEAP. The Local Service Provider provides the client with a letter indicating the amount of the benefit and the utility company to be paid.

9.3 How do you assure that the home energy supplier will charge the eligible household, in the normal billing process, the difference between the actual cost of the home energy and the amount of the payment?

When a crisis, and or heating and cooling payment is made directly to an energy vendor, the vendor shows the amount of the credit on the customer's bill, indicating that the payment was made by LIHEAP. The Local Service Provider provides the client with a letter indicating the amount of the benefit and the utility comapny to be paid.

CSD evaluates the notification process of LIHEAP payments during program evaluation.

A different process is in place for Crisis payments, depending on whether the home energy supplier is a regulated utility or non-regulated one.

Regulated Utilities are audited by the California Public Utilites Comission (CPUC) to ensure that proper billing procedures are in place and the amount of the payments or credits are accurate. No modification of energy rates can occur without a public regulatory process, which is administered by the CPUC.

For Non-Regulated energy vendors:

1. Local Service Providers use a "Confirmation of Payment" form whereby the non-regulated energy vendors records the date and amount credited for each account.

2. Local Service Providers are required to have each home energy supplier sign an assurance agreeing to the requirements of this section. Local Service Providers keep this information on file and clients are advised of their right to fair and equal treatment at the time of service. CSD staff ensures compliance with this provision during program evaluation.

3. Local Service Providers verify, before suppliers for all types of delivered fuels, that the charges for the services and goods provided are reasonable and within fair-market value. The amount of these charges are reviewed during program evaluation.

9.4 How do you assure that no household receiving assistance under this title will be treated adversely because of their receipt of LIHEAP assistance?

Local Service Providers require each home energy supplier to sign an agreement to adhere to the requirements of this assurance. Local Service Providers keep this information on file and clients are advised of their right to fair and equal treatment at the time of service. CSD staff ensures compliance with this provision during program evaluation.

9.5. Do you make payments contingent on unregulated vendors taking appropriate measures to alleviate the energy burdens of eligible households?

○ Yes ◉ No

If so, describe the measures unregulated vendors may take.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 10: Program, Fiscal Monitoring, and Audit, 2605(b)(10)

10.1. How do you ensure good fiscal accounting and tracking of LIHEAP funds?

CSD maintains fiscal controls and accounting practices in accordance with the California Uniform Accounting System. Our financial management system maintains financial data and accounting records supported by source documentation for all federal funds administered. CSD's internal control structure conforms to state and federal procedures. See below for additional information.

Audit Process

10.2. Is your LIHEAP program audited annually under the Single Audit Act and OMB Circular A - 133?

(•) Yes ( ) No

10.3. Describe any audit findings rising to the level of material weakness or reportable condition cited in the A-133 audits, Grantee monitoring assessments, inspector general reviews, or other government agency reviews of the LIHEAP agency from the most recently audited fiscal year.

No Findings ☑

Finding	Type	Brief Summary	Resolved?	Action Taken
1				

10.4. Audits of Local Administering Agencies

What types of annual audit requirements do you have in place for local administering agencies/district offices? Select all that apply.

- ☑ **Local agencies/district offices are required to have an annual audit in compliance with Single Audit Act and OMB Circular A-133**
- ☐ **Local agencies/district offices are required to have an annual audit (other than A-133)**
- ☑ **Local agencies/district offices' A-133 or other independent audits are reviewed by Grantee as part of compliance process.**
- ☑ **Grantee conducts fiscal and program monitoring of local agencies/district offices**

Compliance Monitoring

10.5. Describe the Grantee's strategies for monitoring compliance with the Grantee's and Federal LIHEAP policies and procedures: Select all that apply

Grantee employees:

- ☑ **Internal program review**
- ☑ **Departmental oversight**
- ☑ **Secondary review of invoices and payments**
- ☐ **Other program review mechanisms are in place. Describe:**

Local Administering Agencies / District Offices:

- [x] **On - site evaluation**
- [ ] **Annual program review**
- [x] **Monitoring through central database**
- [x] **Desk reviews**
- [x] **Client File Testing / Sampling**
- [ ] **Other program review mechanisms are in place. Describe:**

10.6 Explain, or attach a copy of your local agency monitoring schedule and protocol.

CSD Field Operations Unit will conduct a combination of in-house and on-site compliance monitoring. In general, CSD's monitoring schedule runs from March 1 - October 31.

Please refer to the CSD's Monitoring Scope for details on the monitoring protocols that will be implemented in the Federal Fiscal Year 2021.

10.7. Describe how you select local agencies for monitoring reviews.

Site Visits:

All LIHEAP agencies have on-site monitoring reviews at least every three years. After conducting an annual risk assessment, the agencies are selected for onsite visits based on the areas of concern identified during the annual risk review, or through whistle blower complaints. Agencies are monitored first with a subsesquent follow up monitoring focusing on the issues identified to ensure full resolution.

Desk Reviews:

CSD will conduct an in-house compliance monitoring of all agencies that do not receive an on-site monitoring visit.

10.8. How often is each local agency monitored ?

At least every 3 years.

10.9. What is the combined error rate for eligibility determinations? OPTIONAL

10.10. What is the combined error rate for benefit determinations? OPTIONAL

10.11. How many local agencies are currently on corrective action plans for eligibility and/or benefit determination issues? 0

10.12. How many local agencies are currently on corrective action plans for financial accounting or administrative issues? 0

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 11: Timely and Meaningful Public Participation, 2605(b)(12), 2605(C)(2)

11.1 How did you obtain input from the public in the development of your LIHEAP plan?
Select all that apply.

- ☐ Tribal Council meeting(s)
- ☑ Public Hearing(s)
- ☑ Draft Plan posted to website and available for comment
- ☐ Hard copy of plan is available for public view and comment
- ☑ Comments from applicants are recorded
- ☑ Request for comments on draft Plan is advertised
- ☑ Stakeholder consultation meeting(s)
- ☐ Comments are solicited during outreach activities
- ☐ Other - Describe:

11.2 What changes did you make to your LIHEAP plan as a result of this participation?

Please see the attached Comment Matrix.

Public Hearings, 2605(a)(2) - For States and the Commonwealth of Puerto Rico Only

11.3 List the date and location(s) that you held public hearing(s) on the proposed use and distribution of your LIHEAP funds?

	Date	Event Description
1		

11.4. How many parties commented on your plan at the hearing(s)?

11.5 Summarize the comments you received at the hearing(s).

Please see the attached Comment Matrix.

11.6 What changes did you make to your LIHEAP plan as a result of the comments received at the public hearing(s)?

Please see the attached Comment Matrix.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 12: Fair Hearings, 2605(b)(13) - Assurance 13

12.1 How many fair hearings did the grantee have in the prior Federal fiscal year? 0

12.2 How many of those fair hearings resulted in the initial decision being reversed? 0

12.3 Describe any policy and/or procedural changes made in the last Federal fiscal year as a result of fair hearings?

There were no changes

12.4 Describe your fair hearing procedures for households whose applications are denied.

Pursuant to Title 22 of the California Code of Regulations, Section 100805, Local Service Providers are required to establish a written appeals process to enable applicants who are denied benefits or services, or who receive untimely response or unsatisfactory performance, the right to appeal the decision or performance to the Contractor. The process must include, at a minimum, all of the requirements of Section 100805 subdivision (b), plus:

1. Provisions that ensure that each applicant is notified in writing of the right to appeal a denial of or untimely response to an application, or to appeal unsatisfactory performance, and the process to request such an appeal, at the time that each applicant submits an application. Such notification shall include information about the right to appeal to both the Contractor and to CSD.
2. Provisions that ensure that Local Service Providers will make a good faith effort to resolve each appeal.
3. Provisions that ensure that Local Service Providers notify the applicant in writing of the Local Service Provider's final decision within 15 working days after the appeal is requested. If the appeal is denied, the written notification must include instructions on how to appeal the decision to CSD. Whenever Local Service Providers notify an applicant of a denial of an appeal, Local Service Providers simultaneously provide a copy of the final decision CSD.
4. Provisions to enable Local Service Providers to collect information on denials and appeals in its regular program reporting.

12.5 When and how are applicants informed of these rights?

Applicants are informed, in writing, regarding the appeal process which is located on the CSD43 Energy Intake Form. Applicants sign and date acknowledgement that they have read and understand their rights to appeal. Additionally, applicants will be able to view their rights to appeal on CSD's public website.

12.6 Describe your fair hearing procedures for households whose applications are not acted on in a timely manner.

During intake, Local Service Providers inform applicants of their right to appeal all claims for assistance that are denied or are not acted upon with reasonable promptness.

1. **Local Service Providers review all claims from applicants who are determined ineligible for benefits or who have submitted written notice that there has been an unreasonable delay in processing their application or receiving their benefits.**
2. **Local Service Providers conduct a fair, and impartial appeals and are required to make a good faith effort to resolve the applicant's complaint(s) at the local level. The Local Service Provider, as a contractor, makes a written finding which sets forth the case of both parties and the decision of the Local Service Provider.**
3. **If the appeal is not resolved at the local level, Local Service Provider informs the applicant that an appeal to the State agency (CSD) may be requested as part of the Fair Hearing process and shall provide the applicant with the appropriate form.**
4. **If the applicant decides to appeal to CSD, the applicant submits a written appeal request to be received by CSD within 10 days from the date of the contracted Local Service Provider's final decision. Upon request from CSD, Local Service Providers provide all supportive documentation to be received by the State via email or postmarked within 5 working days.**
5. **Within 10 working days of receipt of the requested documentation from the contracted Local Service Provider, the CSD Fair Hearing Officer reviews the appeal and supportive documentation, confers with the appellant and the contracted Local Service Provider if necessary, and notifies parties of the hearing. Within 30 days from the date of the hearing, the parties are notified of the Fair Hearing**

Officer's decision in writing.

12.7 When and how are applicants informed of these rights?

Applicants are informed, in writing, regarding the appeals process which is located on the CSD43 Energy Intake Form. Applicants sign and date acknowledgement that they've read and understand their rights to appeal. Additionally, applicants will be able to view their rights to appeal on CSD's public website. The "Filing Appeal" button can be found by clicking on the "Services" tab, then "Help paying your bills".

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 13: Reduction of home energy needs, 2605(b)(16) - Assurance 16

13.1 Describe how you use LIHEAP funds to provide services that encourage and enable households to reduce their home energy needs and thereby the need for energy assistance?

Local Service Providers address the energy needs of low-income households by conducting a thorough energy needs assessment of each client, providing budget counseling, energy conservation education, and coordination with utility companies. Whenever possible, weatherization services are also provided to offer a preventive, holistic and long-term solution to energy needs.

Local Service Providers maintain a source document that substantiates that the client was provided these services. The document is kept on file by the contractor and is reviewed during routine program evaluation.

13.2 How do you ensure that you don't use more than 5% of your LIHEAP funds for these activities?

Up to 5% of the total block grant is allocated specifically for Assurance 16 activities and distributed by formula to the contractor network. CSD provides a budget form for contractors to account for Assurance 16 activities.

Local Service Providers are contractually required to submit monthly expenditure and activity reports to CSD. These reports are monitored cumulatively to ensure that no more than 5% is spent on Assurance 16 activities. The data is entered into an automated database management system, which calculates and verifies compliance. Status reports are printed regularly for use by CSD staff. Issues needing clarification and areas of concern are more readily identified with the automated system that, in turn, allows for a more timely resolution with contractors.

Local Service Providers are made aware of the 5% cap, and through the local planning process, have the flexibility to submit proposed funding levels up to the 5% cap, for activities specifically targeted for Assurance 16.

13.3 Describe the impact of such activities on the number of households served in the previous Federal fiscal year.

The impacts of the budget and energy education are that clients are more aware of their energy and household costs, which may result in overall household savings.

13.4 Describe the level ofdirect benefitsprovided to those households in the previous Federal fiscal year.

N/A

13.5 How many households applied for these services? N/A. CSD does not track the number of applications submitted for LIHEAP assistance.

13.6 How many households received these services? 215942

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 14:Leveraging Incentive Program, 2607(A)

14.1 Do you plan to submit an application for the leveraging incentive program?

(•) Yes ( ) No

14.2 Describe instructions to any third parties and/or local agencies for submitting LIHEAP leveraging resource information and retaining records.

Local Agencies participating in the Leveraging Incentive Program are required to submit a leveraging report to CSD. Agencies are required to retain all support documentation for period of three (3) years.

14.3 For each type of resource and/or benefit to be leveraged in the upcoming year that will meet the requirements of45 C.F.R. § 96.87(d)(2)(iii), describe the following:

Resource	What is the type of resource or benefit ?	What is the source(s) of the resource ?	How will the resource be integrated and coordinated with LIHEAP?
1	Discount/waiver	Utility Companies	Local agencies and CSD coordinate the services provided under LIHEAP with existing reduced rate programs at Californias larger investor-owned utilities, as well as, many smaller municipal utilities. The coordination of these programs enables the agencies to expand services to families who otherwise would not receive assistance due to lack of information about the programs. This coordination occurs through prearranged agreements between the local CSD/LIHEAP contractors and the utility companies. The LIHEAP contractors work in direct conjunction with the utility companies by maintaining ongoing communication to screen and refer potential clients and coordinate benefits. In order to maximize the impact and effectiveness of both programs, applicants are screened to determine if the applicant from either source has already received any benefits. The applicant is provided assistance in completing an application for the reduced rate programs at the time the applicant is being assisted for HEAP.
2	Cash	Non-profits	This resource was integrated and coordinated with LIHEAP in two ways: a. Due to funds from both sources (LIHEAP and utility companies/third-party co-payments) being used in the same household, the low-income household benefited by receiving LIHEAP assistance in addition to assistance from either the utility company program or third-party co-payment once the LIHEAP programs maximum level of assistance was reached. b. To ensure that low-income household have year-around access to energy assistance and that the greatest number of low-income household receive assistance, local agencies have coordinated the services provided under LIHEAP with local private and public energy assistance programs. The coordination of these programs enables the agencies to expand emergency services to families who otherwise would not receive assistance through LIHEAP due to insufficient funds. The coordination occurs through prearranged agreements between the local LIHEAP contractors and the utility assistance providers. The LIHEAP contractors work in direct conjunction with the utility assistance providers by maintaining ongoing communication to screen potential clients and coordinate benefits. In order to maximize the impact and effectiveness of both programs, applicants are screened to determine if any benefits have already been received by the applicant from either source.
3	Cash	Utility companies	Utility companies provide funds to provider agencies, allowing agencies to install additional weatherization measures in qualifying low-income homes.
4	Cash	Utility companies	This resource was integrated and coordinated with LIHEAP due to funds from both sources (LIHEAP and utility companies) being used in the same household. The low-income household, therefore, was further weatherized to prevent the loss of heated and/or cooled air from the dwelling. As a result of the coordination of the weatherization contracts, additional LIHEAP-eligible households received weatherization measures, as appropriate an as allowable within LIHEAP contract.

			The client files are documented and maintained at each respective agency.
5	Cash	Utility companies	This resource is coordinated with LIHEAP because LIHEAP eligible and other low-income households are identified as needing repair or replacement of appliances during the time the dwelling is being assessed for weatherization services. Additionally, the utility companies utilize a bid process to identify administering agencies. CSD-funded agencies are successful in the bid process in large part due to their experience in providing weatherization services under LIHEAP and because they are known entity in the low-income community.
6	In-Kind Contribution	Landlords	Coordination with landlords to provide additional LIHEAP eligible households weatherization and appliances as appropriate and allowable within the LIHEAP contract.
7	Discount/waiver	Local Suppliers	Direct negotiations with local suppliers of weatherization materials for the LIHEAP Program resulted in lower than market costs for materials purchased in bulk quantities. As a result of the resources generated from the discount received from these bulk purchases, additional LIHEAP eligible homes received weatherization measures as appropriate and allowable within the LIHEAP contract.
8	-	-	-

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 15: Training

15.1 Describe the training you provide for each of the following groups:

a. Grantee Staff:

- [x] Formal training on grantee policies and procedures

How often?

- [x] Annually
- [ ] Biannually
- [x] As needed
- [ ] Other - Describe:

- [x] Employees are provided with policy manual
- [ ] Other-Describe:

b. Local Agencies:

- [x] Formal training conference

How often?

- [x] Annually
- [ ] Biannually
- [x] As needed
- [ ] Other - Describe:

- [x] On-site training

How often?

- [ ] Annually
- [ ] Biannually
- [x] As needed
- [ ] Other - Describe:

- [x] Employees are provided with policy manual
- [ ] Other - Describe

c. Vendors

- [ ] Formal training conference

How often?

- [ ] Annually
- [ ] Biannually
- [ ] As needed

☐	**Other - Describe:**
☑	**Policies communicated through vendor agreements**
☐	**Policies are outlined in a vendor manual**
☐	**Other - Describe:**

15.2 Does your training program address fraud reporting and prevention?

- (•) Yes
- ( ) No

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 16: Performance Goals and Measures, 2605(b) - Required for States Only

16.1 Describe your progress toward meeting the data collection and reporting requirements of the four required LIHEAP performance measures. Include timeframes and plans for meeting these requirements and what you believe will be accomplished in the coming federal fiscal year.

CSD has implemented changes to its intake form to meet the required LIHEAP performance measures reporting.

CSD and its Local Service Providers modified its internal/external reporting system to enable CSD's local service providers to transfer data collected from the intake form into CSD's reporting system.

Over the next federal fiscal year, CSD will continue its partnership with Investor Owned Utilities to continue obtaining utility cost and local energy consumption data. CSD will also work with local government utilities and municipal utility companies to obtain data exchange agreement to obtain utility cost and energy consumption data.

If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES

August 1987, revised 05/92,02/95,03/96,12/98,11/01
OMB Clearance No.: 0970-0075
Expiration Date: 09/30/2020

LOW INCOME HOME ENERGY ASSISTANCE PROGRAM(LIHEAP)
MODEL PLAN
SF - 424 - MANDATORY

Section 17: Program Integrity, 2605(b)(10)

17.1 Fraud Reporting Mechanisms

a. Describe all mechanisms available to the public for reporting cases of suspected waste, fraud, and abuse. Select all that apply.

- ☐ **Online Fraud Reporting**
- ☑ **Dedicated Fraud Reporting Hotline**
- ☑ **Report directly to local agency/district office or Grantee office**
- ☐ **Report to State Inspector General or Attorney General**
- ☑ **Forms and procedures in place for local agencies/district offices and vendors to report fraud, waste, and abuse**
- ☑ **Other - Describe:**

CSD operates a toll free line that can be used by the public to report suspected fraud. The Bureau of State Audits has established a whistleblower hotline that is available to grantee staff to report information regarding possible fraud. The information is advertised via posters that are located throughout the department's office. Local administering agencies and vendors report fraud through various methods to the department via correspondence, telephone communication with grantee staff, and email to grantee staff. Upon notification of potential fraud, the department advises its legal office and an investigation commences.

b. Describe strategies in place for advertising the above-referenced resources. Select all that apply

- ☐ **Printed outreach materials**
- ☐ **Addressed on LIHEAP application**
- ☑ **Website**
- ☑ **Other - Describe:**

CSD operates a toll free line that can be used by the public to report suspected fraud. The Bureau of State Audits has established a whistleblower hotline that is available to grantee staff to report information regarding possible fraud. The information is advertised via posters that are located throughout the department's office. Local administering agencies and vendors report fraud through various methods to the department via correspondence, telephone communication with grantee staff, and email to grantee staff. Upon notification of potential fraud, the department advises its legal office and an investigation commences.

17.2. Identification Documentation Requirements

a. Indicate which of the following forms of identification are required or requested to be collected from LIHEAP applicants or their household members.

Type of Identification Collected	Collected from Whom?					
	Applicant Only		All Adults in Household		All Household Members	
Social Security Card is photocopied and retained	☐	Required	☐	Required	☐	Required
	☑	Requested	☐	Requested	☐	Requested
		Required		Required		Required

Social Security Number (Without actual Card)	☐		☐		☐		
	☑	Requested	☐	Requested	☐	Requested	
Government-issued identification card (i.e.: driver's license, state ID, Tribal ID, passport, etc.)	☐	Required	☐	Required	☐	Required	
	☑	Requested	☐	Requested	☐	Requested	

	Other	Applicant Only Required	Applicant Only Requested	All Adults in Household Required	All Adults in Household Requested	All Household Members Required	All Household Members Requested
1		☐	☐	☐	☐	☐	☐

b. Describe any exceptions to the above policies.

17.3 Identification Verification

Describe what methods are used to verify the authenticity of identification documents provided by clients or household members. Select all that apply

- ☐ **Verify SSNs with Social Security Administration**
- ☑ **Match SSNs with death records from Social Security Administration or state agency**
- ☐ **Match SSNs with state eligibility/case management system (e.g., SNAP, TANF)**
- ☐ **Match with state Department of Labor system**
- ☐ **Match with state and/or federal corrections system**
- ☐ **Match with state child support system**
- ☐ **Verification using private software (e.g., The Work Number)**
- ☐ **In-person certification by staff (for tribal grantees only)**
- ☐ **Match SSN/Tribal ID number with tribal database or enrollment records (for tribal grantees only)**
- ☐ **Other - Describe:**

17.4. Citizenship/Legal Residency Verification

What are your procedures for ensuring that household members are U.S. citizens or aliens who are qualified to receive LIHEAP benefits? Select all that apply.

- ☑ **Clients sign an attestation of citizenship or legal residency**
- ☐ **Client's submission of Social Security cards is accepted as proof of legal residency**
- ☐ **Noncitizens must provide documentation of immigration status**
- ☑ **Citizens must provide a copy of their birth certificate, naturalization papers, or passport**
- ☐ **Noncitizens are verified through the SAVE system**
- ☐ **Tribal members are verified through Tribal enrollment records/Tribal ID card**
- ☑ **Other - Describe:**

  County Local Service Providers are required to verify citizenship and legal residency.

17.5. Income Verification

What methods does your agency utilize to verify household income? Select all that apply.

- ☑ **Require documentation of income for all adult household members**
  - ☑ **Pay stubs**
  - ☑ **Social Security award letters**

- [x] **Bank statements**
- [x] **Tax statements**
- [x] **Zero-income statements**
- [x] **Unemployment Insurance letters**
- [ ] **Other - Describe:**

- [ ] **Computer data matches:**
  - [ ] **Income information matched against state computer system (e.g., SNAP, TANF)**
  - [ ] **Proof of unemployment benefits verified with state Department of Labor**
  - [ ] **Social Security income verified with SSA**
  - [ ] **Utilize state directory of new hires**
  - [ ] **Other - Describe:**

17.6. Protection of Privacy and Confidentiality

Describe the financial and operating controls in place to protect client information against improper use or disclosure. Select all that apply.

- [x] **Policy in place prohibiting release of information without written consent**
- [x] **Grantee LIHEAP database includes privacy/confidentiality safeguards**
- [x] **Employee training on confidentiality for:**
  - [x] **Grantee employees**
  - [x] **Local agencies/district offices**
- [x] **Employees must sign confidentiality agreement**
  - [x] **Grantee employees**
  - [x] **Local agencies/district offices**
- [x] **Physical files are stored in a secure location**
- [x] **Other - Describe:**

Statewide Information Management Manual (SIMM) SIMM 5340-C: Requirements to respond to incidents involving breach or personal information

State Administrative Manual (SAM) SAM 5305: Information asset management and all subsections

SAM 5310: Privacy and all subsections and all subsections

SAM 5320: Training and awareness for information security and privacy and all subsections

SAM 5350: Operational Security and all subsections

17.7. Verifying the Authenticity

What policies are in place for verifying vendor authenticity? Select all that apply.

- [ ] **All vendors must register with the State/Tribe.**
- [ ] **All vendors must supply a valid SSN or TIN/W-9 form**
- [x] **Vendors are verified through energy bills provided by the household**
- [ ] **Grantee and/or local agencies/district offices perform physical monitoring of vendors**
- [x] **Other - Describe and note any exceptions to policies above:**

CSD Documents authenticity of regulated energy vendors by collecting the Federal Employer ID number for Gas and Electric Vendors. Vendors are required to submit a Standard 204 Payee Record Data or Government Agency Tax Identification (GATI) form.

17.8. Benefits Policy - Gas and Electric Utilities

What policies are in place to protect against fraud when making benefit payments to gas and electric utilities on behalf of clients? Select all that apply.

- [ ] **Applicants required to submit proof of physical residency**
- [x] **Applicants must submit current utility bill**

- [x] **Data exchange with utilities that verifies:**
  - [ ] **Account ownership**
  - [ ] **Consumption**
  - [x] **Balances**
  - [ ] **Payment history**
  - [x] **Account is properly credited with benefit**
  - [ ] **Other - Describe:**
- [x] **Centralized computer system/database tracks payments to all utilities**
- [x] **Centralized computer system automatically generates benefit level**
- [ ] **Separation of duties between intake and payment approval**
- [ ] **Payments coordinated among other energy assistance programs to avoid duplication of payments**
- [ ] **Payments to utilities and invoices from utilities are reviewed for accuracy**
- [ ] **Computer databases are periodically reviewed to verify accuracy and timeliness of payments made to utilities**
- [x] **Direct payment to households are made in limited cases only**
- [x] **Procedures are in place to require prompt refunds from utilities in cases of account closure**
- [ ] **Vendor agreements specify requirements selected above, and provide enforcement mechanism**
- [x] **Other - Describe:**

  Payments to utilities and direct pay letters are reviewed for accuracy.

17.9. Benefits Policy - Bulk Fuel Vendors

What procedures are in place for averting fraud and improper payments when dealing with bulk fuel suppliers of heating oil, propane, wood, and other bulk fuel vendors? Select all that apply.

- [ ] **Vendors are checked against an approved vendors list**
- [ ] **Centralized computer system/database is used to track payments to all vendors**
- [x] **Clients are relied on for reports of non-delivery or partial delivery**
- [x] **Two-party checks are issued naming client and vendor**
- [x] **Direct payment to households are made in limited cases only**
- [ ] **Vendors are only paid once they provide a delivery receipt signed by the client**
- [ ] **Conduct monitoring of bulk fuel vendors**
- [ ] **Bulk fuel vendors are required to submit reports to the Grantee**
- [ ] **Vendor agreements specify requirements selected above, and provide enforcement mechanism**
- [x] **Other - Describe:**

  Please see attachments.

17.10. Investigations and Prosecutions

Describe the Grantee's procedures for investigating and prosecuting reports of fraud, and any sanctions placed on clients/staff/vendors found to have committed fraud. Select all that apply.

- [x] **Refer to state Inspector General**
- [x] **Refer to local prosecutor or state Attorney General**
- [x] **Refer to US DHHS Inspector General (including referral to OIG hotline)**
- [x] **Local agencies/district offices or Grantee conduct investigation of fraud complaints from public**
- [ ] **Grantee attempts collection of improper payments. If so, describe the recoupment process**
- [ ] **Clients found to have committed fraud are banned from LIHEAP assistance. For how long is a household banned?**
- [ ] **Contracts with local agencies require that employees found to have committed fraud are reprimanded and/or terminated**

☐ **Vendors found to have committed fraud may no longer participate in LIHEAP**
☐ **Other - Describe:**
If any of the above questions require further explanation or clarification that could not be made in the fields provided, attach a document with said explanation here.

Section 18: Certification Regarding Debarment, Suspension, and Other Responsibility Matters

Certification Regarding Debarment, Suspension, and Other Responsibility Matters--Primary Covered Transactions

Instructions for Certification

1. By signing and submitting this proposal, the prospective primary participant is providing the certification set out below.

2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the certification set out below. The certification or explanation will be considered in connection with the department or agency's determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.

3. The certification in this clause is a material representation of fact upon which reliance was placed when the department or agency determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.BrBbr.

4. The prospective primary participant shall provide immediate written notice to the department or agency to which this proposal is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

5. The terms covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549. You may contact the department or agency to which this proposal is being submitted for assistance in obtaining a copy of those regulations.

6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency entering into this transaction.

7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled ``Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction,"

provided by the department or agency entering into this covered transaction, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Nonprocurement Programs.

9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

Certification Regarding Debarment, Suspension, and Other Responsibility Matters--Primary Covered Transactions

(1) The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:

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

(b) Have not within a three-year period preceding this proposal 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;

(c) 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 (1)(b) of this certification; and

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

(2) Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an

explanation to this proposal.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered Transactions

Instructions for Certification

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or had become erroneous by reason of changed circumstances.

4. The terms covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meaning set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this proposal that, [[Page 33043]] should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this proposal that it will include this clause titled ``Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction,'' without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from covered transactions, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Nonprocurement Programs.

8. Nothing contained in the foregoing shall be construed to require

establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Certification Regarding Debarment, Suspension, Ineligibility an Voluntary Exclusion--Lower Tier Covered Transactions

(1) The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

(2) Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

☑ **By checking this box, the prospective primary participant is providing the certification set out above.**

Section 19: Certification Regarding Drug-Free Workplace Requirements

This certification is required by the regulations implementing the Drug-Free Workplace Act of 1988: 45 CFR Part 76, Subpart, F. Sections 76.630(c) and (d)(2) and 76.645(a)(1) and (b) provide that a Federal agency may designate a central receipt point for STATE-WIDE AND STATE AGENCY-WIDE certifications, and for notification of criminal drug convictions. For the Department of Health and Human Services, the central pint is: Division of Grants Management and Oversight, Office of Management and Acquisition, Department of Health and Human Services, Room 517-D, 200 Independence Avenue, SW Washington, DC 20201.

Certification Regarding Drug-Free Workplace Requirements (Instructions for Certification)

1. By signing and/or submitting this application or grant agreement, the grantee is providing the certification set out below.

2. The certification set out below is a material representation of fact upon which reliance is placed when the agency awards the grant. If it is later determined that the grantee knowingly rendered a false certification, or otherwise violates the requirements of the Drug-Free Workplace Act, the agency, in addition to any other remedies available to the Federal Government, may take action authorized under the Drug-Free Workplace Act.

3. For grantees other than individuals, Alternate I applies.

4. For grantees who are individuals, Alternate II applies.

5. Workplaces under grants, for grantees other than individuals, need not be identified on the certification. If known, they may be identified in the grant application. If the grantee does not identify the workplaces at the time of application, or upon award, if there is no application, the grantee must keep the identity of the workplace(s) on file in its office and make the information available for Federal inspection. Failure to identify all known workplaces constitutes a violation of the grantee's drug-free workplace requirements.

6. Workplace identifications must include the actual address of buildings (or parts of buildings) or other sites where work under the grant takes place. Categorical descriptions may be used (e.g., all vehicles of a mass transit authority or State highway department while in operation, State employees in each local unemployment office, performers in concert halls or radio studios).

7. If the workplace identified to the agency changes during the performance of

the grant, the grantee shall inform the agency of the change(s), if it previously identified the workplaces in question (see paragraph five).

8. Definitions of terms in the Nonprocurement Suspension and Debarment common rule and Drug-Free Workplace common rule apply to this certification. Grantees' attention is called, in particular, to the following definitions from these rules:

Controlled substance **means a controlled substance in Schedules I through V of the Controlled Substances Act (21 U.S.C. 812) and as further defined by regulation (21 CFR 1308.11 through 1308.15);**

Conviction **means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the Federal or State criminal drug statutes;**

Criminal drug statute **means a Federal or non-Federal criminal statute involving the manufacture, distribution, dispensing, use, or possession of any controlled substance;**

Employee **means the employee of a grantee directly engaged in the performance of work under a grant, including: (i) All direct charge employees; (ii) All indirect charge employees unless their impact or involvement is insignificant to the performance of the grant; and, (iii) Temporary personnel and consultants who are directly engaged in the performance of work under the grant and who are on the grantee's payroll. This definition does not include workers not on the payroll of the grantee (e.g., volunteers, even if used to meet a matching requirement; consultants or independent contractors not on the grantee's payroll; or employees of subrecipients or subcontractors in covered workplaces).**

Certification Regarding Drug-Free Workplace Requirements

Alternate I. (Grantees Other Than Individuals)
The grantee certifies that it will or will continue to provide a drug-free workplace by:,

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
(b) Establishing an ongoing drug-free awareness program to inform employees about --
(1)The dangers of drug abuse in the workplace;
(2) The grantee's policy of maintaining a drug-free workplace;
(3) Any available drug counseling, rehabilitation, and employee assistance

programs; and
(4) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);
(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will --
(1) Abide by the terms of the statement; and
(2) Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;
(e) Notifying the agency in writing, within ten calendar days after receiving notice under paragraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer or other designee on whose grant activity the convicted employee was working, unless the Federal agency has designated a central point for the receipt of such notices. Notice shall include the identification number(s) of each affected grant;
(f)Taking one of the following actions, within 30 calendar days of receiving notice under paragraph (d)(2), with respect to any employee who is so convicted -(1) Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or
(2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;
(g) Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e) and (f).
(B) The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant:

Place of Performance (Street address, city, county, state, zip code)

2389 Gateway Oaks Drive #100 *** Address Line 1**		
Address Line 2		
Address Line 3		
Sacramento *** City**	CA *** State**	95833 *** Zip Code**

Check if there are workplaces on file that are not identified here.

Alternate II. (Grantees Who Are Individuals)

(a) The grantee certifies that, as a condition of the grant, he or she will not engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance in conducting any activity with the grant;

(b) If convicted of a criminal drug offense resulting from a violation occurring during the conduct of any grant activity, he or she will report the conviction, in writing, within 10 calendar days of the conviction, to every grant officer or other designee, unless the Federal agency designates a central point for the receipt of such notices. When notice is made to such a central point, it shall include the identification number(s) of each affected grant.

[55 FR 21690, 21702, May 25, 1990]

☑ **By checking this box, the prospective primary participant is providing the certification set out above.**

Section 20: Certification Regarding Lobbying

The submitter of this application 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 awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, 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, 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, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, ``Disclosure Form to Report Lobbying,'' 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 subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) 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. Code. 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.

Statement for Loan Guarantees and Loan Insurance

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

If any funds have been paid or will be paid to 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 this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, ``Disclosure Form to Report Lobbying,'' in accordance with its instructions. Submission of this statement is a prerequisite for making or

entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

☑ **By checking this box, the prospective primary participant is providing the certification set out above.**

Assurances

(1) use the funds available under this title to--

(A) conduct outreach activities and provide assistance to low income households in meeting their home energy costs, particularly those with the lowest incomes that pay a high proportion of household income for home energy, consistent with paragraph (5);

(B) intervene in energy crisis situations;

(C) provide low-cost residential weatherization and other cost-effective energy-related home repair;and

(D)plan, develop, and administer the State's program under this title including leveraging programs, and the State agrees not to use such funds for any purposes other than those specified in this title;

(2) make payments under this title only with respect to--

(A) households in which one or more individuals are receiving--

(i)assistance under the State program funded under part A of title IV of the Social Security Act;

(ii) supplemental security income payments under title XVI of the Social Security Act;

(iii) food stamps under the Food Stamp Act of 1977; or

(iv) payments under section 415, 521, 541, or 542 of title 38, United States Code, or under section 306 of the Veterans' and Survivors' Pension Improvement Act of 1978; or

(B) households with incomes which do not exceed the greater of -

(i) an amount equal to 150 percent of the poverty level for such State; or

(ii) an amount equal to 60 percent of the State median income;

(except that a State may not exclude a household from eligibility in a fiscal year solely on the basis of household income if such income is less than 110 percent of the poverty level for such State, but the State may give priority to those households with the highest home energy costs or needs in relation to household income.

(3) conduct outreach activities designed to assure that eligible households, especially households with elderly individuals or disabled individuals, or both, and households with high home energy burdens, are made aware of the assistance available under this title, and any similar energy-related assistance available under subtitle B of title VI (relating to community services block grant

program) or under any other provision of law which carries out programs which were administered under the Economic Opportunity Act of 1964 before the date of the enactment of this Act;

(4) coordinate its activities under this title with similar and related programs administered by the Federal Government and such State, particularly low-income energy-related programs under subtitle B of title VI (relating to community services block grant program), under the supplemental security income program, under part A of title IV of the Social Security Act, under title XX of the Social Security Act, under the low-income weatherization assistance program under title IV of the Energy Conservation and Production Act, or under any other provision of law which carries out programs which were administered under the Economic Opportunity Act of 1964 before the date of the enactment of this Act;

(5) provide, in a timely manner, that the highest level of assistance will be furnished to those households which have the lowest incomes and the highest energy costs or needs in relation to income, taking into account family size, except that the State may not differentiate in implementing this section between the households described in clauses 2(A) and 2(B) of this subsection;

(6) to the extent it is necessary to designate local administrative agencies in order to carry out the purposes of this title, to give special consideration, in the designation of such agencies, to any local public or private nonprofit agency which was receiving Federal funds under any low-income energy assistance program or weatherization program under the Economic Opportunity Act of 1964 or any other provision of law on the day before the date of the enactment of this Act, except that -

(A) the State shall, before giving such special consideration, determine that the agency involved meets program and fiscal requirements established by the State; and

(B) if there is no such agency because of any change in the assistance furnished to programs for economically disadvantaged persons, then the State shall give special consideration in the designation of local administrative agencies to any successor agency which is operated in substantially the same manner as the predecessor agency which did receive funds for the fiscal year preceding the fiscal year for which the determination is made;

(7) if the State chooses to pay home energy suppliers directly, establish procedures to --

(A) notify each participating household of the amount of assistance paid on its behalf;

(B) assure that the home energy supplier will charge the eligible household, in the normal billing process, the difference between the actual cost of the home energy and the amount of the payment made by the State under this title;

(C) assure that the home energy supplier will provide assurances that any agreement entered into with a home energy supplier under this paragraph will

contain provisions to assure that no household receiving assistance under this title will be treated adversely because of such assistance under applicable provisions of State law or public regulatory requirements; and

(D) ensure that the provision of vendor payments remains at the option of the State in consultation with local grantees and may be contingent on unregulated vendors taking appropriate measures to alleviate the energy burdens of eligible households, including providing for agreements between suppliers and individuals eligible for benefits under this Act that seek to reduce home energy costs, minimize the risks of home energy crisis, and encourage regular payments by individuals receiving financial assistance for home energy costs;

(8) provide assurances that,

(A) the State will not exclude households described in clause (2)(B) of this subsection from receiving home energy assistance benefits under clause (2), and

(B) the State will treat owners and renters equitably under the program assisted under this title;

(9) provide that--

(A) the State may use for planning and administering the use of funds under this title an amount not to exceed 10 percent of the funds payable to such State under this title for a fiscal year; and

(B) the State will pay from non-Federal sources the remaining costs of planning and administering the program assisted under this title and will not use Federal funds for such remaining cost (except for the costs of the activities described in paragraph (16));

(10) provide that such fiscal control and fund accounting procedures will be established as may be necessary to assure the proper disbursal of and accounting for Federal funds paid to the State under this title, including procedures for monitoring the assistance provided under this title, and provide that the State will comply with the provisions of chapter 75 of title 31, United States Code (commonly known as the "Single Audit Act");

(11) permit and cooperate with Federal investigations undertaken in accordance with section 2608;

(12) provide for timely and meaningful public participation in the development of the plan described in subsection (c);

(13) provide an opportunity for a fair administrative hearing to individuals whose claims for assistance under the plan described in subsection (c) are denied or are not acted upon with reasonable promptness; and

(14) cooperate with the Secretary with respect to data collecting and reporting under section 2610.

(15) * beginning in fiscal year 1992, provide, in addition to such services as may be offered by State Departments of Public Welfare at the local level, outreach and intake functions for crisis situations and heating and cooling assistance that is administered by additional State and local governmental entities or community-based organizations (such as community action agencies, area agencies on aging and not-for-profit neighborhood-based organizations), and in States where such organizations do not administer functions as of September 30, 1991, preference in awarding grants or contracts for intake services shall be provided to those agencies that administer the low-income weatherization or energy crisis intervention programs.

*** This assurance is applicable only to States, and to territories whose annual regular LIHEAP allotments exceed $200,000. Neither territories with annual allotments of $200,000 or less nor Indian tribes/tribal organizations are subject to Assurance 15.**

(16) use up to 5 percent of such funds, at its option, to provide services that encourage and enable households to reduce their home energy needs and thereby the need for energy assistance, including needs assessments, counseling, and assistance with energy vendors, and report to the Secretary concerning the impact of such activities on the number of households served, the level of direct benefits provided to those households, and the number of households that remain unserved.

Plan Attachments

PLAN ATTACHMENTS
The following documents must be attached to this application
• **Delegation Letter is required if someone other than the Governor or Chairman Certified this Report.**
• **Heating component benefit matrix, if applicable**
• **Cooling component benefit matrix, if applicable**
• **Minutes, notes, or transcripts of public hearing(s).**

Attachment. Section 1 – Program Components

Section 1.2: Estimate what amount of available LIHEAP funds will be used for each component that you will operate: The total of all percentages must add up to 100%.

Re: Weatherization Assistance: 15%

CSD will submit a waiver request pursuant to Federal Regulation: 42 CFR Part 94 §8624(k), to increase the weatherization allocation from 15% to 25%.

Re: Cooling estimate: 6%

For reporting purposes, CSD's cooling season has been determined to be from July 1 through October 31.

Households to be reported under "Cooling" are tied specifically to applicants who have been assisted with their electricity bill under the non-crisis Home Energy Assistance Program (HEAP) component. However, even though the funding estimate for cooling is at 6%, there are additional households that receive assistance during the cooling season under the crisis component, Fast Track, which is reported under "Crisis Assistance". CSD estimates that 8% of the Fast Track funds will be used to help households with their cooling bill. Therefore, CSD estimates that 14% of the households will receive cooling assistance.

Please note: Because the use of non-electric fuels for cooling is rare in California, households assisted with natural gas, wood, propane or other non-electric fuels are not taken into consideration.

Section 5.10 - What is the maximum LIHEAP Weatherization benefit/expenditure per household
The maximum average per dwelling unit will be $7,669 for the 2021 LIHEAP program year.

Section 5.11 - What LIHEAP weatherization measures do you provide ? (Check all categories that apply.)

Other: Describe	Measure
SECTION: Assessments/Diagnostics	
1	Dwelling Assessment
2	REM/Design Energy Audit
3	Combustion Appliance Safety Test
4	Blower Door Test
5	Duct Leakage Test
6	Environmental Testing
7	HERS Rater
8	Permits
9	Contractor Post-Weatherization Inspection
SECTION: Health and Safety	
1	Carbon Monoxide Alarm
2	Smoke Alarm
3	Cooking Appliance Repair, Free Standing Range or Cook Top
4	Cooking Appliance Replacement, Free Standing Range or Cook Top
5	Cooling Repair
6	Cooling Replacement
7	CVA Venting
8	Heating Source Repair
9	Heating Source Replacement
10	Lead-Safe Weatherization
11	Water Heater Repair
12	Water Heater Replacement
SECTION: Mandatory	
1	Attic Ventilation
2	Ceiling Insulation
3	Door, Exterior (All Other Types)
4	Door, Sliding Glass
5	Duct Insulation
6	Duct Repair and Replacement
7	Filter Replacement
8	Hot Water Flow Restrictor
9	Infiltration Reduction (Excludes both repair and replacement of Doors and Windows)
10	Kitchen Exhaust Installation, Repair & Replacement**
11	Kneewall Insulation
12	Lighting
13	Limited Home Repair
14	Low Flow Toilet
15	Mechanical Ventilation (if required by blower door diagnostics and MV calculations)
16	Microwave Oven

Other: Describe	Measure
17	Refrigerator Replacement
18	Thermostat
19	Vacancy Sensor Switch
20	Water Heater Insulation
21	Water Heater Pipe Insulation
22	Whole House Fans
23	Window
SECTION: Optional	
1	Ceiling Fan
2	Exterior Water Pipe Wrap
3	Floor Foundation Venting
4	Floor Insulation
5	Mechanical Ventilation
6	Power Strips
7	Shade screens
8	Shutters
9	Storm Windows
10	Timer, Electric Water Heater
11	Tinted Window Film
12	Wall Insulation, Stucco and Wood
SECTION: Optional - Energy Audit Required	
1	Attic Ventilation
2	Ceiling Insulation
3	Cooling Replacement (Energy Efficiency Upgrades)
4	Door Replacement
5	Duct Insulation
6	Duct Repairs & Replacement
7	Floor Foundation Venting
8	Floor Insulation
9	Heating Source Replacement (Energy Efficiency Upgrades)
10	Infiltration Reduction (Excludes both repair and replacement of Doors and Windows)
11	Kneewall Insulation
12	Limited Home Repair
13	Refrigerator Replacement
14	Shade screen
15	Shutters
16	Storm Window
17	Thermostat
18	Tinted Window Film
19	Water Heater Timer
20	Wall Insulation
21	Water Heater Installation
22	Window

STATE OF CALIFORNIA
Department
of
Community Services and Development

MONITORING SCOPE AND OVERVIEW

Energy & Environmental Services Division

Field Operations Unit

Rev. 5/2020

INTRODUCTION

The Department of Community Services & Development (CSD), as the recipient of the Federal funding, is responsible for oversight of the operations of the Low-Income Home Energy Assistance Program (LIHEAP), the Department of Energy Weatherization Assistance Program (DOE WAP), and other programs as developed within CSD's Energy and Environmental Services Division (E&ESD). As such, CSD is required to monitor the activities of its Contractors (also referred to as 'agency', 'Local Service Provider' or 'subrecipient') and this is accomplished by conducting regular monitoring reviews. The purpose of the reviews is to ensure the Contractor meets the Administrative Requirements, Financial Requirements, Programmatic Requirements, Compliance Requirements, and other applicable requirements as prescribed in the contract and referenced therein (2 C.F.R. §200.328; 45 C.F.R. §75.342; DOE WAP and LIHEAP Part II Subpart D Article 10.3 A-E).

The Department of Energy, as the federal administrator of the Weatherization Assistance Program, requires a comprehensive monitoring review of all DOE agencies every program year. As stated in DOE's Weatherization Program Notices 16-4 & 20-4 and per 10 CFR 440.23, all Weatherization Grantees have the responsibility to perform annual monitoring and oversight of the program implementation and work performed by all of its Subgrantees.

Health and Human Services, as the federal administrator of LIHEAP, requires regular oversight of subrecipients. Per 45 CFR §75.342, CSD "*is responsible for the oversight of the operations of the Federal award supported activities. The non-Federal entity must monitor its activities under Federal awards to assure compliance with applicable Federal requirements and performance expectations are being achieved. Monitoring by the non-Federal entity must cover each program, function or activity.*" Additionally, 45 CFR §75.352 states that CSD must "*monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.*"

MONITORING PLAN

The E&ESD's Field Operations Unit will conduct regular on-site and in-house reviews to verify compliance and work closely with agencies to resolve compliance concerns. An annual analysis will be conducted to help determine which agencies will receive an on-site visit.

LIHEAP Monitoring

All agencies will receive a comprehensive on-site monitoring review once every three years. CSD will select agencies for review based on a rotating schedule and every year, 13 to 14 agencies will receive an on-site visit. At the end of the third year, all 41 agencies will have received an on-site visit.

On-site client file reviews will consist of:

- A minimum of 20-40 files from the Utility Assistance (HEAP & Fast Track), and Wood, Propane and Oil (ECIP & HEAP WPO) components.
- 5% (or at least 5 files) review of Weatherization and ECIP Emergency Heating and Cooling client files
    - 5% will be based on the dwelling projections identified on the CSD 622 LIHEAP Production Plan or actual dwellings reported, whichever is higher.
- Sampling of SWEATS client files, for agencies who have provided SWEATS services.

LIHEAP agencies who do not have a DOE program will instead be monitored via a Quarterly Review, in-house, for the year(s) they are not scheduled to have an on-site visit. This quarterly review will include a review of UA and WPO client files (a minimum of 20-40 files).

In the event an on-site review cannot be conducted due to issues outside of our control (such as COVID-19), a comprehensive desk review will be done in lieu of an on-site or the on-site visit will be postponed until it is deemed possible.

DOE Monitoring

Each year, agencies with a DOE contract will receive a comprehensive review conducted via onsite at the agency or in-house at CSD. If a LIHEAP agency scheduled for an on-site visit also has a DOE contract, the visit will be a comprehensive review of both programs. In the year(s) agencies are not scheduled to have an on-site visit for LIHEAP, their DOE program will be monitored in-house via a Desk Review and Quarterly Reviews.

A minimum of 5% of DOE client files (or 5 files, whichever is greater) will be reviewed for compliance; unless otherwise required (e.g., minimum 10% review per 2017 DOE Addendum B or significant compliance issues identified). The percentage to be reviewed will be based on the dwelling projections identified on the CSD 622D DOE WAP Performance and Expenditure Benchmark or actual dwellings reported, whichever is higher.

In the event an on-site review cannot be conducted due to issues outside of our control (such as COVID-19), a comprehensive desk review will be done in lieu of an on-site or the on-site visit will be postponed until it is deemed possible.

Types of Monitoring Reviews

On-site Reviews are conducted at the Local Service Provider's location (also referred to as 'monitoring visit' or 'on-site monitoring'). The On-site Review predominantly consists of verification of processes and activities such as, but not limited to, administrative policy review, financial line item reconciliation, client file verification, etc. Specific documents will be requested in advance with the Monitoring Questionnaire, in an effort to reduce the amount of time spent on-site and to allow CSD Field Representatives the opportunity to identify any deficiencies in order to prepare for any Training and Technical Assistance (T&TA) that will be provided while on-site. A listing of client files to be reviewed on-site will be identified and requested from the agency no less than five (5) business days prior to the on-site monitoring visit. Depending on the outcome of the review, CSD Field Representatives may expand the sampling size to determine whether the issue is isolated or systemic. Lastly, CSD Field Representatives will also verify that all previous in-house (desk and quarterly reviews) and On-site Review issues have been resolved during the on-site monitoring visit.

Desk Reviews are conducted yearly, in-house at CSD, in lieu of an On-site Review for the DOE program and will predominantly consist of verification of processes and activities such as, but not limited to, administrative policy review, client file verification, etc. Specific documents will be requested by the agency with the Monitoring Questionnaire. Additionally, CSD Field Representatives will request documentation, such as client files, to be submitted via CSD's FTP site to complete the Desk Review. Depending on the outcome of the client file review, CSD Field Representatives may expand the sampling size to determine whether the issue is isolated or systemic. Lastly, CSD Field Representatives will also verify that all previous in-house (desk and quarterly reviews) and On-site Review issues have been resolved during the desk review.

Quarterly Reviews are conducted in-house at CSD on a quarterly basis and focus on expenditure status, follow up on CSD 558s, SWEATS, etc., and will be one of the tools used to assist in formulating the monitoring strategy for on-site visits or in-house desk reviews.

Recommendations, Observations, and Findings

CSD strives to maintain the highest levels of performance through a monitoring process that has the following goals:

- To ensure proper and timely use of funds and realization of expected benefits;
- To provide transparency and accountability;
- To provide quality control;
- To provide training and technical assistance; and
- To confirm corrective action implementation for prior Findings and Observations.

In an effort to provide transparency, the CSD Field Representatives will be identifying "POTENTIAL" Recommendations, Observations, and/or Findings throughout the on-site monitoring visit and during the on-site monitoring Exit Conference, as well as at the conclusion of the Desk Review. However, the ultimate determination will be made following the two-week review period of the draft monitoring report and will be reflected in the final monitoring report. Although the basic premise is to "standardize" the Monitoring process, the uniqueness of each agency and circumstances at the time of the visit will impact the ultimate outcome of the final Monitoring Review.

This section outlines the issues identified during the reviews. Those issues are categorized into three (3) categories: Recommendations, Observations, and Findings.

'**Recommendations**' are offered by CSD as a suggestion for (1) potential improvement of current processes, systems, or general business practices OR (2) may result in an Observation and/or Finding if not improved. Please note that 'Recommendations' do not require a Corrective Action Plan response.

'**Observations**' are identified contractual noncompliance issues that are an identified 'Significant Deficiency' which is caused by a deficiency, or combination of deficiencies, in internal control that is less severe than a 'Material Weakness,' yet important enough to merit attention (*i.e. Missing or incomplete documents with no financial impact and is a federal and/or state requirement*). An Observation does not require a Corrective Action Plan response; however, the agency must immediately remedy the issue of noncompliance within 90 calendar days from the issuance of the final monitoring report. Thus, if the agency fails to document the remediation of and/or forsakes to remedy an 'Observation' by the specified timeframe, upon follow up the 'Observation' may then be elevated to a 'Finding' as it now carries material error.

'**Findings**' are identified contractual noncompliance issues that: (1) cause a financial impact (*i.e. Missing the required Post-Wx Inspection documentation to substantiate inspection was performed*); OR (2) was a previously identified Observation and/or Finding that was not found to be remedied; OR (3) is a Material Weakness caused by a deficiency or combination of deficiencies in internal control, such that there is a reasonable possibility of a material misstatement that will not be prevented, or detected and corrected on a timely basis. Findings are considered material noncompliance of the contract, and any materials referenced therein. A material noncompliance is defined as any issue which carries substantial financial, personnel, public, and/or agency/CSD ramifications; a material noncompliance may or may not preclude the agency from further performance. Please note that 'Findings' require a Corrective Action Plan from the agency within 30 calendar days of the issue of the final report outlining how the issue of noncompliance will be remedied and other course of action as outlined in each topic.

MONITORING SCOPE

I. ADMINISTRATIVE REQUIREMENTS

A. ADMINISTRATIVE POLICIES AND PROCEDURES

1. Board Roster, By Laws, Resolution and Minutes
2. Internal Controls Requirements
3. Record Retention Requirements
4. Travel and per diem
5. Codes of Conduct
6. Conflict of Interest
7. Procurement Standards
8. Use and Disposition of Vehicles and Equipment
9. Subcontracts (CSD)
10. Complaint Management Policies and Procedures
11. Fair Hearing Process for Applications for Denial of Benefits by Contractor
12. Fraud, Waste and Abuse

II. FINANCIAL REQUIREMENTS

A. ADMINISTRATIVE AND PROGRAM EXPENDITURES REQUIREMENTS

1. Working Capital Advance and Major Purchase Advances
2. Program Income
3. Wood, Propane and Oil Returned Payments
4. Allowable Costs
5. Reimbursement Guidelines

B. REPORTING POLICIES AND PROCEDURES

1. Reporting Requirements

III. PROGRAMMATIC REQUIREMENTS

A. PROGRAM POLICIES AND PROCEDURES
B. PROGRAM IMPLEMENTATION
C. TRAINING, LICENSING AND CERTIFICATIONS

IV. COMPLIANCE REQUIREMENTS

A. PROGRAM POLICIES AND PROCEDURES

MONITORING SCOPE OVERVIEW

The general scope for CSD's Energy & Environmental Services Division's monitoring includes, but is not limited to, the following areas:

I. ADMINISTRATIVE REQUIREMENTS

A. ADMINISTRATIVE POLICIES AND PROCEDURES

1. Board Roster, By Laws, Resolution and Minutes
LIHEAP & DOE WAP Part II Subpart A Article 4.1

The purpose of this review is to ensure that the agencies are in compliance with their By Laws and that the Board is regularly updated with any impactful Energy Program issues.

- **i.** CSD Field Representatives will review the Board Minutes to verify that Board Meetings are being held in accordance with the Board By Laws, Board Meeting Minutes are being submitted to CSD, and whether Energy Programs are being discussed during meetings.

2. Internal Controls Requirements
2 C.F.R. 200.61-62; 2 CFR 200.313; LIHEAP & DOE WAP Part II Subpart A Article 4.2

The purpose of this review is to ensure the agency has appropriate safeguards in place for inventory and property purchased with federal funds and if the agency regularly conducts internal reviews.

- **i.** CSD Field Representatives will review the agency's response(s) provided in the Monitoring Questionnaire.

3. Record Retention Requirements
2 C.F.R. 200.333-337; 45 CFR 75.361; LIHEAP & DOE WAP Part II Subpart A Article 4.3

The purpose of this review is to ensure the agency retains records (financial, equipment, employee, and client) for at least three (3) years after the close-out of the contracts, or any audits or legal proceedings, and that those records are maintained in a secure and confidential manner.

- **i.** CSD Field Representatives will review the agency's response(s) provided in the Monitoring Questionnaire and its Record Retention policy to verify the agency is abiding by OMB requirements for retention.

4. Travel and Per Diem
2 C.F.R. 200.474; 45 CFR 75.474; C.C.R. 599.615-638; LIHEAP & DOE WAP Part II Subpart A Article 4.6

The purpose of this review is to ensure the agency follows its written travel policy, or is abiding by the California Code of Regulations.

i. CSD Field Representatives will review the agency's response(s) provided in the Monitoring Questionnaire and utilize the EARS database to verify if the agency has any out-of-state travel expenses budgeted, if any costs have been incurred, and will request to review the agency's CSD 536 forms (Out-of-State Travel).

5. Codes of Conduct

2 C.F.R. 200.318; LIHEAP & DOE WAP Part II Subpart A Article 4.7

The purpose of this review is to ensure the agency follows its written Codes of Conduct policy.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and its Codes of Conduct policy.

6. Conflict of Interest

2 C.F.R. 200.112, 200.318; LIHEAP & DOE WAP Part II Subpart A Article 4.8

The purpose of this review is to ensure the agency, if electing to provide CSD services to employees, officers, board members, and/or friends and family, has a process in place that prevents the appearance of preferential treatment, and is adhering to the notification and approval procedure as prescribed in the contract.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and its Conflict of Interest Policy and Procedure. If services were provided to agency employees, relatives of employees, board members and/or officers, CSD Field Representatives will review those files to ensure preferential treatment was avoided.

7. Procurement Standards

2 C.F.R. 200.317-326; 45 C.F.R. 75; CPA-A-12-01; LIHEAP & DOE WAP Part II Subpart A Article 4.9

The purpose of this review is to ensure the agency's Procurement Policy and Procedures are in compliance with the OMB Uniform Guidance including, but not limited to, open and free competition including a cost analysis.

i. CSD Field Representatives will review the agency's responses to the Monitoring Questionnaire, and its Procurement Policy and Procedure. On an on-going basis, CSD Field Representatives will review any CSD 558 Request for Pre-Approval of Purchase/Lease to follow-up on obtaining proof of purchase.

ii. CSD Field Representatives will test the agency's procurement process via a review of the agency's subcontractor procurement or other item(s) procured with LIHEAP and/or DOE funds. If CSD Field Representatives have any questions on the procurement of materials, equipment, and/or subcontractors, supporting documentation may be requested, and agency staff may be interviewed for further clarification.

8. Use and Disposition of Vehicles and Equipment
2 C.F.R. 200.311, 200.313, 200.436; 45 C.F.R. 75.320; CPN-A 17-01; LIHEAP & DOE WAP Part II Subpart A Article 4.10

The purpose of this review is to ensure the agency's Use and Disposition Policy and Procedures are in compliance with the OMB Uniform Guidance including, but not limited to, use of vehicles, user fees, property logs, and limitation on use of funds.

i. CSD Field Representatives will review the agency's responses to the Monitoring Questionnaire, its property log and compliance with the use, maintenance and disposition of vehicles and equipment purchased with LIHEAP and/or DOE funds.

9. Subcontracts (CSD)
2 CFR 200.300-331; LIHEAP & DOE WAP Part II Subpart A Article 4.11

The purpose of this review is to ensure the agency's Subcontractor Agreements are in compliance with all contract requirements, proper procurement was conducted, adequate oversight is in place, and that CSD was notified timely of any new agreements.

i. CSD Field Representatives will review the agency's response(s) to the Questionnaire, its Subcontractor Oversight Policy, and all energy Subcontractor Agreements, including the original solicitation and procurement process.

ii. CSD Field Representatives will review weatherization client files to verify proper subcontractor documentation is within the file, that reimbursement rates are being adhered to, and that there is proper oversight of the subcontractors.

10. Complaint Management Policies and Procedures
LIHEAP & DOE WAP Part II Subpart A Article 4.12

The purpose of this review is to ensure the agency has established policies and procedures for handling complaints, applicants are afforded an opportunity to register a complaint, the agency offers a reasonable remedy within the contract timeframes, and formal written complaints are documented.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire, its Complaint Management Policy and Procedure, 15-day notification letter, and formal complaint tracking log.

11. Fair Hearing Process for Applications for Denial of Benefits by Contractor

22 C.C.R. 100805; 22 C.C.R. 100904.5; LIHEAP & DOE WAP Part II Subpart A Article 4.13

The purpose of this section is to ensure the agency has a written appeals process in place providing applicants who are denied benefits or services, or who receive an untimely response or unsatisfactory performance, the right to appeal.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and its Appeals Process.

12. Fraud, Waste and Abuse

2 C.F.R. 200.113, 31 U.S.C. 3321, 41 U.S.C. 2313; LIHEAP & DOE WAP Part II Subpart A Article 4.14

The purpose of this review is to ensure the agency has a system in place to notify CSD of incidents and activities, including suspected incidents and activities, involving the fraud, waste and/or abuse of Energy Program funds.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and will verify the agency has provided necessary information to their employees, subcontractors, clients, and other parties regarding contact information to report actual or suspected fraud, waste, and/or abuse.

II. FINANCIAL REQUIREMENTS

A. ADMINISTRATIVE AND PROGRAM EXPENDITURES REQUIREMENTS

1. Working Capital Advance and Major Purchase Advances

2 C.F.R. 200.305(b)(8), 22 C.C.R. 100840(a), 100855; LIHEAP Part II Subpart B Article 5.3 and DOE WAP Part II Subpart B Article 5.2

The purpose of this review is to ensure the agencies requesting Working Capital Advances (WCA) and/or Major Purchase Advances (MPA) are placing the funds in an interest-bearing account.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and will request a copy of the interest-bearing account bank statement.

2. **Program Income**
2 C.F.R. 200.307, 22 C.C.R. 100855(c); CPN-A-18-01; LIHEAP Part II Subpart B Article 5.4 and DOE WAP Part II Subpart B Article 5.3

The purpose of this review is to ensure the agency maintains records of the receipt and disposition of all Program Income.

i. CSD Field Representatives will review the agency's response(s) to the Monitoring Questionnaire and review prior Close-Out Reports for reported Program Income.

3. **Wood, Propane and Oil Returned Payments**
LIHEAP Part II Subpart B Article 5.5

The purpose of this review is to determine if the agency has a system in place for tracking returned Wood, Propane and Oil (WPO) payments in accordance with tracking requirements.

i. CSD Field Representatives will review the agency's responses to the Monitoring Questionnaire and their submitted WPO Tracking Log.

4. **Allowable Costs**
DOE Weatherization Program Notice 16-4; LIHEAP Part II Subpart B Article 5.6 and DOE WAP Part II Subpart B Article 5.4

The purpose of this review is to determine whether the agency is claiming reimbursements for actual, allowable and allocable costs.

i. CSD Field Representatives will review the responses to the Monitoring Questionnaire.

ii. For agencies scheduled to receive an on-site visit, CSD Field Representatives will perform a financial line item reconciliation of reported costs for selected line items and months.

a. In the event an on-site review cannot be conducted due to issues outside of our control (such as COVID-19), the Field Representative may elect to perform financial line item reconciliation during a desk review.

5. **Reimbursement Guidelines**
42 U.S.C. 8622(1), CPN 12-05; LIHEAP Part II Subpart B Article 5.8 and DOE WAP Part II Subpart B Article 5.6

The purpose of this review is to ensure the agency is reporting measures within the allowable maximums, is not reporting dwellings until after they have been fully inspected, the average cost per dwelling is within the contract limits, and the client file contains the required applicable documentation.

i. CSD Field Representatives will review client files to ensure the dwelling was post inspected prior to billing, the files contain the applicable required documentation and that the reimbursement amount shall be equal to the actual labor costs and actual cost of the materials and that subcontracted services do not exceed the maximum reimbursement allowable.

B. REPORTING POLICIES AND PROCEDURES

1. Reporting Requirements

2 C.F.R. 200.305, 200.343, CPN-E 19-002; LIHEAP & DOE WAP Part II Subpart B Article 6.1

The purpose of this review is to ensure the agency is submitting expenditures regularly and that expenditures reported are accompanied by the measure information submitted to the Weatherization Database.

i. CSD Field Representatives will review CSD's EARS Receipt and Approval spreadsheet to verify expenditure submissions, and the Weatherization Database to verify measure submission.

III. PROGRAMMATIC REQUIREMENTS

A. PROGRAM POLICIES AND PROCEDURES

CPN-E 16-01; CPN-E 18-001; LIHEAP & DOE Part II Subpart C Articles 7.1-7.7.8

The purpose of this review is adhering to the Program Standards and Regulatory Requirements, is conducting a Prioritization of Services, is adhering to the Outreach and Intake Activity Guidelines and Assurance 16 Guidelines, is documenting Leveraging Activities, and is maintaining records in accordance to the Record Keeping Responsibilities states within the contracts.

i. CSD Field Representatives will review the agency's responses to the Monitoring Questionnaire regarding programmatic requirements and will request and review client files, utilizing the Client File Checklist to confirm that all files contain the applicable documentation as stated within the contracts. Additionally, a comparison between the client files and the client data submitted to the Weatherization Database will be conducted.

B. PROGRAM IMPLEMENTATION
10 C.F.R. 440.22(b)(2), 16 U.S.C.470, 36 C.F.R. 60.4; LIHEAP & DOE WAP Part II Subpart C Articles 8.1-8.6

The purpose of this review is to confirm the agency's ECIP, HEAP and Weatherization activities are done in accordance with the contract terms and the agency's Local Plan and Priority Plan Narrative.

i. CSD Field Representatives will review client files, utilizing the Client File Checklist, to confirm that the agency is following the contract and Field Guide programmatic requirements, including conducting 100% post inspections. Additionally, a review will be conducted to ensure adequate separation of duties and that subcontracted DOE QCI services are not exceeding the maximum amount as specified in the contract.

C. TRAINING, LICENSING AND CERTIFICATIONS
LIHEAP & DOE WAP Part II Subpart C Articles 9.1-9.5

The purpose of this review is to confirm if that the agency's staff, including subcontractors and/or subrecipients, has received the appropriate training for their job duties as outlined in the contract, and has the appropriate certifications such as Quality Control Inspector (QCI), Contractor Licensing and Environmental Protection Agency (EPA) Certifications.

i. CSD Field Representatives will review the completed matrices within the Monitoring Questionnaire to confirm the agency has staff trained for all weatherization job duties listed and has the appropriate licenses and certifications to perform weatherization work. Additionally, client files will be reviewed to confirm work is being performed by trained staff.

IV. COMPLIANCE REQUIREMENTS

A. EXPENDITURE AND PRODUCTION REQUIREMENTS
LIHEAP & DOE WAP Part II Subpart D Article 10.5

The purpose of this review is to verify whether the agency is meeting their expenditure and unit production goals and that expenditures are in compliance with the contract requirements.

i. CSD Field Representatives will review the agency's expenditure status and compare the results to the agency's submitted CSD 622 Performance and Expenditure Benchmark and Performance Plan.

INFORMATION SECURITY PROGRAM MANAGEMENT **5305.1**
(Revised 8/2015)

Policy: Each state entity must provide for the proper use and protection of its information assets. Accordingly each state entity shall:

1. Develop, implement, and maintain a state entity-wide Information Security Program Plan.
2. Ensure the plan documentation provides the following:
    a. an overview of the requirements for the state entity's information security program;
    b. a description of the state entity's strategy and prioritization approach to information security, privacy, and risk management;
    c. a plan for integrating information security resource needs into the state entity's capital planning and funding request processes; and
    d. a plan of action and milestones (POAM) process for addressing program deficiencies. State entities shall use the standardized POAM reporting instructions and tool (SIMM 5305-B and SIMM 5305-C, respectively).
3. Ensure the plan is approved and disseminated by the state entity head responsible and accountable for risks incurred to the state entity's mission, functions, assets, image and reputation.
4. Identify roles and responsibilities, and assign management responsibilities for information security program management consistent with the roles and responsibilities described in the Information Security Program Management Standard (SIMM 5305-A).

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A); Plan of Action and Milestones (SIMM 5305-B and SIMM 5305-C)

POLICY, PROCEDURE AND STANDARDS MANAGEMENT 5305.2

(Revised 6/14)

Policy: Each state entity must provide for the protection of its information assets by establishing appropriate administrative, operational and technical policies, standards, and procedures to ensure its operations conform with business requirements, laws, and administrative policies, and personnel maintain a standard of due care to prevent misuse, loss, disruption or compromise of state entity information assets. Each state entity shall adopt, maintain and enforce internal administrative, operational and technical policies, standards and procedures in accordance with SIMM 5305-A to support information security program plan goals and objectives.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); SIMM 5305-A

INFORMATION SECURITY ROLES AND RESPONSIBILITIES 5305.3

(Revised 6/14)

Policy: Information security is a shared responsibility. All personnel have a role and responsibility in the proper use and protection of state information assets. Each state entity shall ensure information security program roles and responsibilities identified in SIMM 5305-A are acknowledged and understood by all state entity personnel.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); SIMM 5305-A

PERSONNEL MANAGEMENT 5305.4

(Revised 12/13)

Policy: Each state entity must identify security and privacy roles and responsibilities for all personnel. This will ensure personnel are informed of their roles and responsibilities for using state entity information assets, to reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include:

1. Employment history, fingerprinting, and/or criminal background checks on personnel who work with or have access to confidential, personal, or sensitive information or critical applications may be necessary for a particular state entity. Each state entity should consult the California Human Resources Department and the Department of Justice for specific rules and regulations relative to employment history, fingerprinting, or criminal background checks.
2. Initial training of state entity personnel with respect to individual, state entity, and statewide security and privacy responsibilities and policies before being granted access to information assets, and annually thereafter.
3. Signing of acknowledgments of security and privacy responsibility by all personnel.
4. Transfer procedures that ensure access rights and permissions to state entity information assets are reviewed for appropriateness and reauthorized by program management when personnel is transferred within the state entity, so that access to information assets is limited to that which is needed by personnel in the performance of their job-related duties.
5. Termination procedures that ensure state entity information assets are not accessible to separated personnel.

INFORMATION ASSET MANAGEMENT **5305.5**
(Revised 6/14)

Introduction: In order to provide for the proper use and protection of information assets, the value and level of protection needed must be clearly specified and understood.

Policy: Each state entity must understand the value of its information assets and the level of protection those assets require. To this end, each state entity shall establish and maintain an inventory of all of its information assets, including information systems, information system components, and information repositories (both electronic and paper). The inventory shall contain a listing of all programs and information systems identified as collecting, using, maintaining, or sharing state entity information. The inventory must include categorization and classification of the information assets by program management, and based on the Information Security Program Management Standard (SIMM 5305-A), California Public Records Act (Government Code sections 6250-6265), Information Practices Act of 1977 (Civil Code Section 1798, et seq.), FIPS Publication 199, and laws governing administration of the state entity's programs.

The categorization and classification of information assets shall be used in the determination of an asset's needed level of protection. If the information asset's level of protection is not clear, the state entity is to protect the asset to the categorization level of "Moderate" as defined by FIPS Publication 199. Where the state entity is the custodian or user of the information asset, and not the owner, as in the case of Federal Tax Information, Criminal Justice Information Services information, and so forth the state entity shall ensure the data owner specifies the level of protection. The state entity shall adhere to the data owner's classification and level of protection requirements.

Each information asset for which the state entity has ownership responsibility shall be inventoried and identified to include the following:

1. Description and value of the information asset.
2. Owner of the information asset.
3. Custodians of the information asset.
4. Users of the information asset.
5. Classification of information.
6. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).

(Continued)

(Continued)
INFORMATION ASSET MANAGEMENT **5305.5** (Cont. 1)
(Revised 6/14)

7. Importance of information asset to the execution of the state entity's mission and program function.
8. Potential consequences and impacts if confidentiality, integrity and availability of the information asset were compromised.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); Information Security Program Management Standard (SIMM 5305-A); and FIPS Publication 199.

RISK MANAGEMENT 5305.6

(Revised 6/14)

Policy: Each state entity shall create a state entity-wide information security, privacy and risk management strategy which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the state entity's risk tolerance, and approaches for monitoring risk over time.

The state entity's risk management strategy and methodologies shall be consistent with NIST SP 800-30 and NIST SP 800-39, and must include:

1. Risk assessments conducted at the three various levels of the risk management hierarchy, including:
    a. Organizational level;
    b. Mission/Business process level; and
    c. Information asset level.
2. A risk assessment process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks; including, but not limited to:
    a. Risk associated with introducing new information processes, systems and technology into the state entity environment;
    b. Accidental and deliberate acts on the part of state entity personnel and outsiders;
    c. Fire, flooding, and electric disturbances; and,
    d. Loss or disruption of data communications capabilities.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM); and SIMM 5305-A

RISK ASSESSMENT **5305.7**
(Revised 6/14)

Policy: Each state entity shall conduct 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/asset and the information it processes, stores, or transmits. Each state entity shall conduct a comprehensive risk assessment once every two years which assesses the state entity's risk management strategy for all three levels and documents the risk assessment results in a risk assessment report.

The risk assessment process must include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
2. Identification of the state entity information assets that are at risk, with particular emphasis on the applications of information technology that are critical to state entity program operations. Identification of the threats to which the information assets could be exposed.
3. Assessment of the vulnerabilities, e.g., the points where information assets lack sufficient protection from identified threats.
4. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
5. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
6. Selection of cost-effective security management measures to be implemented.
7. Preparation of a report, to be submitted to the state entity head and to be kept on file within the state entity, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity.

Implementation Controls: NIST SP 800-53: Risk Assessment (RA)

PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES 5305.8

(Revised 6/14)

Introduction: State entities are required to enter into written agreements with state and non-state entities when they engage such entities in the development, use, or maintenance of information systems, products, solutions, or services.

Policy: Each state entity shall ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state. Agreements shall include, at a minimum, provisions which cover the following:

1. Appropriate levels of security (confidentiality, integrity and availability) for the data based on data categorization and classification and FIPS Publication 199 protection levels.
2. Standards for transmission and storage of the data, including encryption and destruction, if applicable.
3. Agreements to comply with statewide policies and laws regarding the use and protection of information resources and data, including those set forth in this Chapter.
4. Signed confidentiality statements.
5. Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
6. Agreements to notify the state data owners promptly if a security incident involving the information system or data occurs.
7. Agreements that the data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation, and that data custodian shall cooperate fully in such investigations.

(Continued)

(Continued)
PROVISIONS FOR AGREEMENTS WITH STATE AND NON-STATE ENTITIES **5305.8** (Cont. 1)
(Revised 6/14)

8. Agreements that the data custodian shall be responsible for all costs incurred by the data owner due to security incident resulting from the data custodian's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the data owner. If the data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.
9. Agreements that the data custodian shall immediately notify and work cooperatively with the data owner to respond timely and correctly to public records act requests.
10. Agreements between the data custodian and data owner to address the appropriate disposition of records held by the data custodian during the term of its agreement with the data owner.

Implementation Controls: NIST SP 800-53, System and Services Acquisition (SA)

INFORMATION SECURITY PROGRAM METRICS 5305.9

(Revised 6/14)

Introduction: Performance with respect to security controls must be measured to determine whether the needs of the state entity are being met. Security metrics assist with adjustments to security controls in order to improve effectiveness.

Policy: Each state entity shall establish outcome-based metrics to measure the effectiveness and efficiency of the state entity's information security program, and the security controls deployed.

Implementation Controls: NIST SP 800-53: System and Services Acquisition (SA); Security Assessment and Authorization (CA); Contingency Planning (CP)

INFORMATION SECURITY PROGRAM 5305

(Revised 6/14)

Policy: Each state entity is responsible for establishing an information security program. The program shall include planning, oversight, and coordination of its information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets.

Each state entity shall:

1. Align the information security program, its activities, and staff with the requirements of this Chapter;
2. Establish a governance body to direct the development of state entity specific information security plans, policies, standards, and other authoritative documents;
3. Oversee the creation, maintenance, and enforcement of established information security policies, standards, procedures, and guidelines;
4. Ensure the state entity's security policies and procedures are fully documented and state entity staff is aware of, has agreed to comply with, and understands the consequences of failure to comply with policies and procedures;
5. Identify and integrate or align information security goals and objectives to the state entity's strategic and tactical plans;
6. Develop and track information security and privacy risk key performance indicators;
7. Develop and disseminate security and privacy metrics and risk information to state entity executives and other managers for decision making purposes; and
8. Coordinate state entity security efforts with local government entities and other branches of government as applicable.

Implementation Controls: NIST SP 800-53: Planning (PL); Program Management (PM)

STATE ENTITY PRIVACY STATEMENT AND NOTICE ON COLLECTION 5310.1

(Revised 6/14)

Policy: Information asset owners shall be open about state entity information handling practices, including the purposes for which the state entity collects, uses, and discloses personal information of individuals. Each state entity Privacy Program Coordinator shall prepare, publish, and maintain a General Privacy Policy Statement and a Privacy Notice on Collection for each personal information collection in accordance with the Privacy Statement and Notices Standard (SIMM 5310-A).

General Privacy Policy Statement

Each state entity's general privacy policy, as required by Government Code section 11019.9, shall apply to the entire state entity and its subdivisions.

Privacy Notice on Collection

When personal information is collected from an individual on or with any form, the information asset owner shall ensure that notice is provided to the individual at or before the time of collection. The content and presentation of the notice shall comply with requirements outlined in the Privacy Statement and Notices Standard (SIMM 5310-A).

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-A

LIMITING COLLECTION 5310.2

(Revised 6/14)

Policy: Information asset owners shall collect the least amount of personal information that is required to fulfill the purposes for which it is being collected. Information asset owners shall obtain personal information only through lawful means and shall collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source. Information asset owners shall endeavor to collect non-personal information, instead of personal information, if it is able to fulfill the same requirements.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

LIMITING USE AND DISCLOSURE 5310.3

(Revised 6/14)

Policy: Information asset owners, custodians and users shall not disclose, use, or make available personal information collected from individuals for purposes other than those for which it was originally collected, except in the following situations:

1. The disclosure is made to the individual who is the subject of the information;
2. The nature of the disclosure is included in the Privacy Notice on Collection provided at or before the time of collection;
3. The individual who is the subject of the information, subsequent to collection, provides explicit consent to the disclosure or use; or
4. The use or disclosure is explicitly allowed under Civil Code section 1798.24.

Accounting of Disclosures

Information asset owners shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made under exception number 4 above. The accounting shall include the date of the disclosure, and the name, title, and business address of the individual or state entity to which the disclosure was made.

Information asset owners shall retain the above referenced accounting for at least three years after the disclosure for which the accounting is made, or until the record is destroyed in accordance with the state entity record retention policy, whichever is shorter.

Information asset owners shall inform any individual or state entity to whom a record containing personal information has been disclosed during the preceding three years of any correction of an error in the record or notation of a dispute about its accuracy.

Use of Information by Third Parties

Information asset owners and users shall apply the requirements of this policy to any third party who handles personal information collected by the state entity, in order to accomplish a state entity function that is consistent with the original purposes for which it was collected. Any such third party and its personnel or agent with access to the personal information shall formally agree to be subject to the state entity's privacy policies and practices in the same manner as an employee of the state entity.

(Continued)

(Continued)
LIMITING USE AND DISCLOSURE **5310.3 (Cont. 1)**
(Revised 6/14)

Social Security Numbers
Information asset owners shall minimize the collection and use of Social Security numbers. Information asset owners shall not publicly post or publicly display in any manner an individual's Social Security number or otherwise permit handling of Social Security numbers in any manner inconsistent with the Privacy Individual Access Standard (SIMM 5310-B).

Information asset owners shall not permit Social Security numbers to be either entered into systems as authentication credentials or used as user unique identifiers within systems. This requirement shall apply to all new systems, and major changes or upgrades to existing systems.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-B

INDIVIDUAL ACCESS TO PERSONAL INFORMATION 5310.4

(Revised 6/14)

Policy: Each state entity shall ensure individuals are provided with information about their access rights and the procedures for exercising those rights.

Individuals Right to Access

Each state entity Privacy Program Coordinator shall publish procedures for individuals to follow in exercising their rights to access records held by the state entity which contain their personal information. Such rights include the right to inquire and be informed as to whether the state entity maintains a record about the individual and the right to request a correction of or an amendment to their personal information. Such procedures shall be made available online if the state entity has a website, and shall otherwise comply with the Privacy Individual Access Standard (SIMM 5310-B).

Personal Information in Public Records

Each state entity head shall include in the state entity's procedures for access to public records, a provision requiring the redaction of personal information prior to allowing inspection or releasing records in response to a California Public Records Act request.

Mailing Lists

Upon written request of an individual, an information asset owner maintaining a mailing list shall remove the individual's name and contact information from such list, unless such name and contact information is exclusively used by the state entity to directly contact the individual. Information asset owners shall inform individuals, in the requisite Privacy Notice on Collection forms used to collect personal information, of their right to have their information removed from such mailing lists.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog , and SIMM 5310-B

INFORMATION INTEGRITY 5310.5

(Revised 6/14)

Policy: Information asset owners shall maintain all records with accuracy, relevance, timeliness, and completeness.

Maintaining Record Integrity

When an information asset owner uses a record to make a determination about an individual or transfers a record to another state or non-state entity, the owner shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or out of date.

Maintaining Information Sources

Whenever an information asset owner collects personal information, the owner shall either ensure that the individual is provided a copy of the source document or shall record and maintain the source of the information, unless the source is the individual record subject.

Ownership of Stored Records and State Archived Records

1. Stored Records: When records that contain personal information are transferred to the Department of General Services (DGS) for storage, information asset owners for the state entity transferring the records shall retain all owner responsibilities for the protection of the record as provided in this Chapter. The DGS shall not disclose the record except to the information asset owner or his designee, or in accordance with their instructions which must be in accordance with this policy and relevant laws.
2. State Archives: Information asset owners shall transfer a record pertaining to an identifiable individual to the State Archives only after determining, with concurrence by the state entity head, that the record has sufficient historical or other value to warrant its continued preservation by the California state government. In the event of this transfer, information asset ownership shall be formally transferred to an information asset owner in the State Archives, who shall accept all owner responsibilities contained in the enterprise information security and privacy policies and standards.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

DATA RETENTION AND DESTRUCTION 5310.6

(Revised 6/14)

Policy: Information asset owners shall retain and/or destroy records of personal information in accordance with the state entity's record retention and destruction policy and the Privacy Individual Access Standard (SIMM 5310-B). Information asset owners shall take reasonable steps to keep personal information only as long as is necessary to carry out the purposes for which the information was collected.

However, no record of personal information shall be destroyed or otherwise disposed of by any state entity unless:

a. It is determined by the state entity head that the record has no further administrative, legal, or fiscal value;
b. The state entity head has determined that an audit has been performed for any record subject to audit; and
c. The Secretary of State has determined that the record is inappropriate for preservation in the State Archives.

Destruction of Electronically Collected Personal Information

An information asset owner shall, upon request by the record subject, securely discard without reuse or distribution, any personal information collected through a state entity's website.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog, and SIMM 5310-B

SECURITY SAFEGUARDS 5310.7

(Revised 6/14)

Policy: Information asset owners shall apply all applicable statewide and state entity information security laws, policies, standards, and procedures in order to protect personal information under the information asset owner's responsibility.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

PRIVACY **5310**
(Revised 6/14)

Introduction: Privacy can be understood as the rights of individuals, as defined by law, to control the collection and use of their personal information. This privacy policy is based generally on the Information Practices Act of 1977 (Civil Code section 1798, et seq.). In addition to its general application, the Information Practices Act of 1977 is broad in scope, drawing from the Fair Information Practice Principles (FIPPs), which form the basis for most privacy laws in the United States and around the world. The FIPPs help entities attain public trust and mitigate loss and risk stemming from privacy incidents.

Included among the principles are transparency, notice, and choice. Some state entities are also subject to additional state and federal privacy laws related to particular types of personal information.

Governing Authority: The following overarching privacy laws are applicable to state entities:

1. Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.

2. The Information Practices Act of 1977 (Civil Code section 1798, et seq.) places specific requirements on each state entity in the collection, use, maintenance, and dissemination of information relating to individuals.

3. Government Code Section 11019.9 requires state agencies to enact and to maintain a privacy policy and to designate an employee to be responsible for the policy. The policy must describe the agency's practices for handling personal information, as further required in the Information Practices Act.

Policy: State entity heads shall direct the establishment of an entity-specific Privacy Program. The Privacy Program shall ensure, and privacy coordinators shall confirm, that the requirements contained in the California Information Practices Act, this policy and the associated standards are adhered to by the state entity and its personnel.

Implementation Controls: NIST SP 800-53: Appendix J-Privacy Control Catalog

SECURITY AND PRIVACY AWARENESS 5320.1

(Revised 12/13)

Policy: Each state entity shall provide basic security and privacy awareness training to all information asset users (all personnel, including managers and senior executives) as part of initial training for new users and annually thereafter.

Each state entity shall determine the appropriate content of security awareness training based on statewide requirements, specific state entity requirements, and the information processes and assets to which personnel have access.

SECURITY AND PRIVACY TRAINING 5320.2

(Revised 6/14)

Policy: Each state entity shall determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security requirements of the state entity and the information assets to which personnel have access. Privacy training content will ensure personnel understand their responsibility for compliance with the Information Practices Act of 1977 and the penalties for non-compliance.

Governing Provisions: Civil Code section 1798

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

SECURITY AND PRIVACY TRAINING RECORDS **5320.3**
(Revised 6/14)

Policy: Each state entity shall document and monitor individual information security and privacy training activities including basic security and privacy awareness training and specific information system security training; and retain individual training records to support corrective action, audit and assessment processes. The ISO will be responsible for ensuring that training content is maintained and updated as necessary to address the latest security challenges that may impact users.

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

PERSONNEL SECURITY **5320.4**
(Revised 6/14)

Policy: Each state entity shall establish processes and procedures to ensure that individual access to information assets is commensurate with job-related responsibilities, and individuals requiring access to information assets sign appropriate user agreements prior to being granted access.

Access agreements shall include acceptable use provisions, and may also include nondisclosure agreements and conflict-of-interest agreements. If required by law, regulation or policy, each state entity must ensure individuals obtain applicable security clearances.

Personnel transfers or reassignments to other positions within the state entity must be reviewed to prevent accumulation of access and support least access privilege. Returning and issuing keys, identification cards, and building passes; closing information system accounts and establishing new accounts; and changing information system access authorizations are all examples of personnel security practices related to staff transfer or reassignment.

Implementation Controls: NIST SP 800-53: Personnel Security (PS)

TRAINING AND AWARENESS FOR INFORMATION SECURITY AND PRIVACY 5320

(Revised 6/14)

Policy: Each state entity must establish and maintain an information security and privacy training and awareness program. State entity personnel must possess the knowledge and skills necessary to use information technology to the best advantage for the state. Each state entity must regularly assess the skills and knowledge of its personnel in relation to job requirements, identify and document training and professional development needs, and provide suitable training within the limits of available resources.

The training and awareness program shall ensure:

1. All personnel receive general security and privacy awareness training so that they understand the state entity information security policies, standards, procedures, and practices; and are knowledgeable about the various management, operational, and technical controls required to protect the information assets for which they are responsible.
2. Groups of personnel with special security training needs, such as application developers receive the necessary training.
3. Training records are maintained to support corrective action, audit and assessment processes.
4. The program content is maintained and evaluated for effectiveness on an ongoing basis.

State entity heads, Chief Information Officers (CIOs), ISOs, management, and information asset owners have key roles in information security training and awareness. The state entity head is responsible for ensuring an effective program is implemented state entity-wide. The scope and content of the awareness program must align with statewide policy, and with any state entity specific security needs and requirements.

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)

ENCRYPTION **5350.1**
(Revised 6/14)

Policy: End-to-end encryption or approved compensating security control(s) shall be used to protect confidential, sensitive, or personal information that is transmitted or accessed outside the secure internal network (e.g., email, remote access, file transfer, Internet/website communication tools) of the state entity, or stored on portable electronic storage media (e.g., USB flash drives, tapes, CDs, DVDs, disks, SD cards, portable hard drives), mobile computing devices (e.g., laptops, netbooks, tablets, and smartphones), and other mobile electronic devices. In rare instances where encryption cannot be implemented, compensating control(s) or alternatives to encryption must be in place. Compensating controls and alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the state entity ISO, after a thorough risk analysis.

Implementation Controls: FIPS 140-2, FIPS 197, NIST SP 800-53: Access Control (AC), and System and Communications Protection Controls (SC)

OPERATIONAL SECURITY 5350

(Revised 6/14)

Introduction: In order to mitigate against successful attacks, each state entity is responsible for separating and controlling access to various systems and networks with different threat levels and sets of users which may operate or interface within their technology environment.

Policy: Each state entity shall develop, implement, and document, disseminate, and maintain operational security practices which include, but are not limited to:

1. A network security architecture that:
    a. includes distinct zones to separate internal, external, and DMZ traffic; and
    b. segments internal networks to limit damage, should a security incident occur.
2. Firewall, router, and other perimeter security tools which enforce network security architecture decisions.
3. Periodic review of perimeter security access control rules to identify those that are no longer needed or provide overly broad access.

Each state entity's security architecture shall align with the following security controls and best practices:

1. Application partitioning;
2. Denial of service protection;
3. Boundary protection;
4. Confidentiality of transmitted information or appropriate compensating security controls if protection assurances cannot be guaranteed; and
5. Cryptographic protections using modules that comply with FIPS-validated cryptography.

Implementation Controls: NIST SP 800-53: System and Information Integrity (SI); System and Communications Protection (SC)

State of California

California Department of Technology

Office of Information Security

Requirements to Respond to Incidents Involving a Breach of Personal Information

SIMM 5340-C

January 2018

REVISION HISTORY

Revision	Date of Release	Owner	Summary of Changes
Initial Release		California Office of Information Security (CISO)	
Minor Update	May 2012	CISO	Added Attorney General requirements pursuant to Civil Code Section 1798.29€. effective 1/2012.
Minor Update	December 2012	CISO	Name change to shortened document title, added additional examples under the section *A. Whether Breach Notification Is Required by Law,* and replaced reference to contacting California Office of Privacy Protection for assistance with use of Credit Monitoring Services with reference to published guidance.
Minor Update	September 2013	CISO	SIMM number change, replaced reference to California Office of Privacy Protection in the Sample Breach Notices.
Minor Update	January 2014	CISO	Added new notice triggering data elements and notification requirements to coincide with enacted Legislation.
Update	January 2016	CISO	Added new notice triggering data elements and notification requirements to coincide with enacted Legislation (Civil Code Sections 1798.29, 1798.82).
Minor Update	April 2016	CISO	Non-substantial change to breach notification templates clarifying signature requirements per SAM 5300.3 and adding hyperlink to Breach Help pages.
Minor Update	June 2016	CISO	Update incident reporting instructions for the SIMM 5340-B: eliminating incident reporting through ENTAC; directing all incident reports to be made through the Cal-CSIRS system.
Update	March 2017	CISO	Added reporting/notification requirements to include breach of encrypted personal information to coincide with enacted Legislation (Civil Code Section 1798.29).
Minor Update	January 2018	Office of Information Security (OIS)	Office name change

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Agencies/state entities are required to operate in accordance with a myriad of laws and state policies related to the protection of information assets, and the timely and efficient management of security incidents. California's breach notification law (Civil Code Section 1798.29), enacted in 2002, is one such law, intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so they could take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact and other possible harms associated with a breach of personal information.

While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led to the addition of medical and health insurance information as "notice-triggering" in 2008. In 2015 the addition of a user name or e-mail address, in combination with a password or security question that would permit access to an online account, was added to the list. In 2016, encrypted personal information acquired by an unauthorized person with access to the encryption key or security credential and the Automated License Plate Recognition System were added as "notice-triggering" elements. Safeguarding against and preventing security breaches involving personal information entrusted to government is essential to establishing and maintaining public trust. Equally important is the ability to provide accurate and timely information about a breach to affected individuals when a breach occurs because failure to do so can exacerbate the problem and increase the risk of harm to individuals.

To ensure that agencies/state entities understand the responsibilities for making timely and accurate notification to individuals affected by a breach, this SIMM 5340-C document identifies the existing personal information breach notification requirements, and sets out specific instructions and guidance for agencies/state entities to follow when responding to a security incident that involves a breach of personal information. This document also provides a checklist and a set of breach notification templates as tools to assist agencies/state entities with fulfilling the notification requirements.

II. INTRODUCTION

To ensure compliance and consistency across state government, this document identifies the current breach notification requirements for breaches involving personal information, accompanied by questions and factors agencies/state entities should consider in determining whether and when a breach notification should be made, and a specification of the means for fulfilling notification requirements. This document does not attempt to establish an absolute standard for breach notification, since decisions are dependent upon the specific facts surrounding the breach and the applicable law. In some cases notification is clearly required by law, and in others it may be unclear whether notification is required. In some instances, where notification is, by law, clearly not required, notification may nonetheless, serve the best interests of those affected.

The procedures discussed in this document will assist agencies/state entities in confronting the problems associated with a breach involving personal information, by providing instruction and guidance regarding developing an appropriate response, understanding notification requirements, and making decisions in cases where the obligation to notify may be uncertain.

The term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this document, "agency" and "department" are used interchangeably.

III. INFORMATION PRACTICES ACT REQUIREMENTS

A. Background

The California Information Practices Act (IPA) of 1977 (Civil Code Sections 1798 et seq.) is the primary authority that governs state agencies' collection, use, maintenance, and dissemination of individuals' personal information. The IPA also specifies the circumstances that compel breach notification.

For the general purposes of the IPA, Civil Code Section 1798.3 defines personal information very broadly as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, Social Security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

B. Breach Notification Requirement

Subdivision (a) of Civil Code Section 1798.29, requires "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable". For purposes of this section, encrypted has been defined as "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security". For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render the data useable, readable, and decipherable.

The breach notification section of the IPA, subdivision (g) of Civil Code Section 1798.29, more narrowly defines, "personal information" as the following:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

    a. Social Security number.
    b. Driver's License number or California Identification Card number.
    c. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    d. Medical information (as defined in Civil Code Section 1798.29).
    e. Health insurance information (as defined in Civil Code Section 1798.29).
    f. Automated License Plate Recognition (ALPR) System Information (as defined in Civil Code Section 1798.90.5).

2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Subdivisions (h) (1) through (3) of Civil Code Section 1798.29 specifically define personal information, medical information, and health information for purposes of this section as follows:

1. For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Note; however, personal information held in public records, or portions thereof, may need to be redacted prior to disclosure to comply with Civil Code Section 1798.24).

2. For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

3. For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Subdivisions (b) and (d) of Civil Code Section 1798.90.5 specifically defines the ALPR System and the information received through the use of the ALPR Systems as follows:

1. ALPR system means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

2. ALPR information means information or data collected through the use of an ALPR system.

For purposes of this document the elements of personal information described in subdivisions (e) and (f) of Civil Code Section 1798.29 are hereinafter referred to as "notice-triggering" data elements.

Effective January 1, 2016, Civil Code Section 1798.29 subsections (1) (A through E), specified formatting requirements for the breach notification letters and subsections (2) (A through F) specified content requirements.

Further, effective January 1, 2012, Civil Code Section 1798.29 (e), requires any agency that is required to issue a security breach notification to more than 500 California residents as a result of a single breach to electronically submit a sample copy of the breach notification, excluding any personally identifiable information, to the Attorney General. The Attorney General's procedures for sample submission are available on its website at: http://oag.ca.gov/ecrime/databreach/reporting

IV. STATE POLICY REQUIREMENTS

A. Information Processing Standards

State policy, in accordance with State Administrative Manual (SAM) Section 5100, requires agencies/state entities to use the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. The ANSI standards are national consensus standards that provide guidance on a variety of issues central to the public and industrial sectors. Under the Information Technology Management Reform Act (Public Law 104-106). The Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) as FIPS for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

In relation to Civil Code Section 1798.29's exemption from the breach notification requirement for a breaches involving encrypted notice-triggering information, this requirement, includes without limitation, those NIST standards related to the validation of cryptographic modules found in **encryption products used in the protection of confidential, personal, or sensitive information.** The exemption is only applicable to those incidents involving data encrypted with products validated by NIST as FIPS 140-2 compliant.

B. Incident Management

State policy (SAM Section 5340) requires agency management to promptly investigate incidents involving loss, damage, misuse of information assets, unauthorized access, or improper dissemination of information, and immediately report the occurrence of such incidents to the Office of Information Security (OIS) and the California Highway Patrol (CHP), through the California Compliance and Security Incidents Reporting System (Cal-CSIRS). Detailed incident reporting procedures can be found in the Incident Reporting and Response Instructions (SIMM 5340-A).

Proper incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

In conjunction with the aforementioned requirements, SIMM 5340-A requires every state agency that collects, uses, or maintains personal information to include in their incident management plan, procedures for responding to a security breach involving personal information **regardless of the medium in which the breached information is held** (e.g., paper, electronic, oral, or the combination of data elements involved including non-notice-triggering personal information). These procedures must be documented and must address, at a minimum, the following:

1. Agency Incident Response Team. An agency's procedures shall identify the positions responsible for responding to a security breach involving personal information. An agency's response team must include, at a minimum, the following:

   - an escalation manager,
   - the Program Manager of the program or office experiencing the breach,
   - the Information Security Officer (ISO),
   - the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy,
   - the Public Information or Communications Officer,
   - Legal Counsel, and
   - others as directed by OIS.

   The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved, and are driving the process to completion. Some incidents will require the involvement of other persons not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. As another example, if the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves a compromise of state employee's personal information, the Personnel Officer or Human Resources Manager should also be involved in the response activity.

   Further, if the incident involves multiple agencies/state entities, the response team from each agency/state entity may be involved.

2. Protocol for Escalation, Internal Reporting, and Response. An agency's procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that the agency's executive management is informed about the breach of personal information, the Agency Incident Response Team is assembled, and the incident is addressed in the most expeditious and efficient manner.

   An initial impact assessment and response coordination meeting, attended by all response team personnel, is highly recommended when a security incident involves notifying a large number of individuals, involves multiple agencies/state agencies, or is likely to garner media attention. This meeting clarifies roles, responsibilities, and timelines for incident reporting and response activities.

   When multiple agency personnel are involved; attendee and sign-in rosters are used to track participant involvement. Non-disclosure agreements may also be used to ensure confidential information remains confidential and communications do not compromise or complicate an active investigation.

3. Protocol for Security Incident Reporting. Any actual or suspected incident meeting the criteria described earlier or breach of personal information (notice- triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to OIS and CHP through Cal- CSIRS. Representatives from the OIS and/or CHP's Computer Crime Investigation Unit (CCIU) will contact the state entity as soon as possible following their receipt of the Cal-CSIRS notification.

IMPORTANT: A report made to CHP, other law enforcement agencies, or the OIS outside of the Cal-CSIRS notification process by email or other means is NOT an acceptable substitute for the required report through Cal- CSIRS.

In the case that the Cal-CSIRS system is offline during normal business hours, contact OIS directly by phone at (916) 445-5239 or by e-mail at security@state.ca.gov for assistance. If the Cal-CSIRS system is offline outside of normal business hours and you require immediate law enforcement assistance, contact CHP's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will forward that information to CCIU for immediate assistance. In the situation that notification is made outside of normal business hours through CHP, it is the state entity's responsibility to notify OIS of incident the next business day.

A state entity report must outline the details of the incident and corrective actions taken, or to be taken, to address the root cause of the incident. The report must be completed through Cal-CSIRS within 10 business days following creation of the incident. If corrective actions cannot be completed immediately, follow the instructions outlined in Plan of Action and Milestones Instructions (SIMM 5305-B) to submit a Plan of Actions and Milestones (SIMM 5305-C) that identifies all corrective actions along with timelines indicating when these corrective actions will be completed. If the state entity currently has a POAM on file, you will need to update the existing POAM and resubmit.

4. Decision-Making Criteria and Protocol for Notifying Individuals.
   Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies/state entities to resolve a number of questions. An agency's procedures shall include documentation of the methods and manner for determining when and how notification is to be made.

   To assist agencies with navigating the decision-making process, a checklist is provided as Appendix A, Breach Response and Notification Assessment Checklist. The procedures shall, at a minimum, address the following elements:

   a. Whether the notification is required by law.
   b. Whether the notification is required by state policy.
   c. Timeliness of notification.
   d. Source of notice.
   e. Content of notice.
   f. Approval of notice prior to release.
   g. Method(s) of notification.
   h. Preparation for follow-on inquiries.
   i. Other actions that agencies/state entities can take to mitigate harm to individuals.
   j. Other situations when notification should be considered.

   A more detailed description of these elements is set forth in the following section.

V. ESSENTIAL ELEMENTS TO CONSIDER

A. Whether Breach Notification Is Required by Law

California's Breach Notification Law (Civil Code Section 1798.29) requires "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable".

The law is intended to give individuals early warning when their personal information is reasonably believed to have been acquired by an unauthorized person, so that those individuals can take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact. While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led, in 2008, to the addition of medical and health insurance information as notice-triggering information. In 2015 the addition of a user name or e-mail address, in combination with a password or security question that would permit access to an online account, was also added to the list. Most recently, the Automated License Plate Recognition (ALPR) System was determined to have the ability to store personal identifiable information and was added as a "notice-triggering" element in 2016.

To determine whether notification of a breach is required by law, the agency should consult with their legal counsel. Note, other sector specific laws and regulations may also require notification, such as laws governing Federal Tax Information (FTI), and the Health Information Portability and Accountability Act (HIPAA). Answering the following questions should assist the agency and its legal counsel in making the determination as it relates to Civil Code Section 1798.29:

1. Was computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved computerized data, the agency is to consider, at a minimum, whether the data involved was processed or stored with or in a computer or computer system. This includes, but is not limited to, copier, facsimile and business hub machines, mobile telephone and portable digital assistant (PDA) devices, data processed or stored with or in electronic mail systems, online accounts, and data collected through an ALPR system.

2. Was a computer system, or computer peripheral, or storage device with the capability of storing computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved a computer system, or computer peripheral, or storage device with capability of storing computerized data the agency is to consider the wide array of data storage devices available today.

This includes, but is not limited to, those mentioned above, as well as USB flash, jump or pen drives, CDs and DVDs, external and removable hard drives, and magnetic and optical backup tapes/disks.

3. Were notice-triggering data elements involved?

   a. In accordance with Civil Code Section 1798.29, notice triggering data elements include an individual's first name or first initial and last name in combination with any one or more of the following:

      i. Social Security number.
      ii. Driver's License number or California Identification Card number.
      iii. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
      iv. Medical information (as defined in Civil Code Section 1798.29).
      v. Health insurance information (as defined in Civil Code Section 1798.29).
      vi. ALPR System information (as defined in Civil Code Section 1798.90.5).

   b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

4. Were the notice-triggering data elements encrypted using FIPS 140-2 validated or NIST certified cryptographic modules?

   The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standards (FIPS 140-2 and others). An alphabetical list of vendors who have implemented NIST validated cryptographic modules list is available on NIST's CMVP website at http://csrc.nist.gov/groups/STM/cmvp/validation.html

   FIPS 140-2 precludes the use of invalidated cryptography **for the cryptographic protection** of sensitive or valuable data. Invalidated cryptography is viewed by NIST as providing **no protection** to the information or data - in effect the data would be considered unprotected plaintext.

5. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

   When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider, at a minimum, the following indicators:

   a. The information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information, or such as a misdirected electronic mail transmission received and opened by an unauthorized person containing notice-triggering information.

b. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred which may require forensic analysis);
c. The attacker deleted security logs or otherwise "covered their tracks";
d. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting;
e. The attack vector is known for seeking and collecting personal information;
f. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.

B. Whether Breach Notification Is Required by State Policy

The compromise of notice-triggering data elements found in physical information systems poses the same level of risk to individuals as a compromise of notice-triggering data elements found in computerized systems; thus, state policy requires notification be made to individuals in these cases, as well. To determine whether notification is **required** by state policy, the agency should still consult with its legal counsel. However, answering the following questions, which are a slight variation to those above, should assist the agency and its legal counsel in making this determination:

1. Was data, on **any other media type or format** (e.g., paper, cassette tape), owned or licensed by the state agency involved?

2. Were notice-triggering data elements involved?

   a. In accordance with Civil Code Section 1798.29, notice triggering data elements include an individual's first name or first initial and last name in combination with any one or more of the following:

      i. Social Security number.
      ii. Driver's License number or California Identification Card number.
      iii. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
      iv. Medical information (as defined in Civil Code Section 1798.29).
      v. Health insurance information (as defined in Civil Code Section 1798.29)
      vi. (ALPR System information (as defined in Civil Code Section 1798.90.5).

   b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

   When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider the following indicators:

   a. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information. This includes, but is not limited to, documents containing notice-triggering data elements which have been

addressed and mailed to an unauthorized person, transmitted by facsimile to an unauthorized person, or information containing notice-triggering data elements which is otherwise conveyed, such as by word-of-mouth, to unauthorized persons.

b. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.

c. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported, or fraudulent accounts opened.

C. Timeliness of the Notification

Following the discovery of a breach that involves personal information which meets the statutory or policy criteria for notification, agencies/state entities should provide notification to affected individuals in a timely manner and without unreasonable delay.

To the extent possible, notification should be made within ten (10) business days from the date the agency has determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person. The following are examples of circumstances which may warrant the delay of notification beyond the 10 days following discovery:

- Legitimate needs of law enforcement, when notification would impede or compromise a criminal investigation, or pose other security concerns [Civil Code Section 1798.29 (c)].
- Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system, so that the harm of the initial incident is not compounded by premature announcement. For example, if a data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident. [Civil Code Section 1798.29 (a)].

Any decision to delay notification should be made by the agency head, or the senior- level individual designated in writing by the agency head as having authority to act on his/her behalf, and any delay should not exacerbate the risk of harm to any affected individual(s).

D. Source of the Notification

Given the serious security and privacy concerns raised by breaches involving personal information, the notice to individuals affected by the loss should be issued and signed by a responsible official of the agency. In those instances in which the breach involves a widely known component of an agency, notification should be given by a responsible official of the component. In general, notification to individuals affected by the breach should be issued by the agency head, or by the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf. Such action, demonstrates that the incident has the attention of the chief executive of the organization.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the breach involves a contractor operating a system of records on behalf of the agency or a

public-private partnership. The roles, responsibilities, and relationships with contractors or partners for complying with notification procedures should be established in writing with the contractor or partner prior to entering the business relationship, and must be reflected in the agency's breach response plan and in the contractual agreements with those entities.

Whenever practical, to avoid creating confusion and anxiety for recipients of the notice, the notice should come from the entity that the affected individuals are more likely to perceive as the entity with which they have a relationship. In all instances, when the breach involves a contractor or a public-private partnership operating a system on behalf of the agency, the agency is responsible for providing any required or necessary notification, and for taking appropriate corrective actions.

E. Format of the Notification

The breach notification shall be designed to call attention to the nature and significance of the information it contains, and shall be formatted on official letterhead to include:

1. No smaller than 10-point Ariel font type;

2. A title “Notice of Data Breach”; and

3. Contain at a minimum the following headings:

   a. “What Happened”
   b. “What Information Was Involved”
   c. “What We Are Doing”
   d. “What You Can Do”
   e. “Other Important Information”
   f. “For More Information”

F. Content of the Notification

The substance of the notice should be written in clear, concise, and easy-to-understand language. The notice should avoid the use of technical jargon and shall include, at a minimum, the following elements:

1. A general description of what happened; including the date of breach if known; if not known, the estimated date or date range within which the breach occurred. Agencies/state entities should be mindful of the impact of disclosing either an insufficient amount of detail or too much detail in the general description of what happened. For example, in cases where an investigation is ongoing, disclosing certain details may impede or compromise the investigation, or cause other security concerns. On the other hand, failure to disclose a sufficient amount of detail may not provide the recipient with enough information to fully understand and mitigate their own risk. An agency must work with law enforcement authorities to ensure the content strikes the necessary balance.

2. A description of the type of personal information involved in the breach (e.g., full name, Social Security number, Driver’s License number or California Identification

   Card number, date of birth, home address, account number, disability code, medical

or health information (as defined), etc.). The specific type of notice-triggering data elements are to be provided in the notice. This is extremely important in order to help the recipient of the notice to fully understand how to mitigate their risk.

3. All of the steps that the individual could take to protect themselves from potential harm, if any.

4. An apology and a description of the steps the agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches.

5. The name and contact information of the individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.

6. A toll-free telephone number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free telephone number a local telephone number may be provided.

When the agency has knowledge that the affected individuals are not English speaking, to the extent practical, the notice should also be provided in the appropriate language(s). Given the amount of information required above, in cases where it is only the name and Social Security number that has been breached, agencies/state entities may want to consider using the one-page *Breach Help –Consumer Tips from the California Attorney General* document as an enclosure with the notice letter. It is available in English and in Spanish and can be downloaded at: http://www.privacy.ca.gov/consumers/index.shtml.

The *Breach Help –Consumer Tips from the California Attorney General* document, as well as standardized breach notification templates for breaches involving other notice-triggering information, is provided as appendices (B through K) in this document. In some cases it may be necessary to combine the language from multiple templates, such as in the hybrid template provided.

Consistent with Section 504 of the Rehabilitation Act of 1973, the agency should also give special consideration in providing notice to individuals who are visually or hearing impaired. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's Web site.

G. Approval of the Notification

SIMM 5340-A requires agencies/state entities to submit draft breach notices to OIS for review and approval **prior to their release**. The intent is to ensure the consistency and clarity of notices, as well as the accuracy of privacy protection steps and instructions provided in notices. The procedures for submitting a request for review and approval of a draft breach notice to the OIS are as follows:

1. **Communicate with OIS security representative by telephone at (916) 445-5239 immediately prior to submission of any document, in order to alert the Office that a document requiring review will soon arrive.**

2. Upload breach notification, with corresponding incident report (SIMM 5340-B), into

Cal-CSIRS. Cal-CSIRS procedures can be found in the SIMM 5340-A.

3. Indicate the target date of release. Allow at least one full business day for OIS's review and approval of the initial and any subsequent submittals that are necessary due to changes not previously reviewed and approved by OIS.

Depending on the circumstances, the agency may also need to contact other public and private sector agencies, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, an agency may need to seek confirmation from law enforcement that notification will not compromise the investigation. Or, when as a result of a large breach in individual names and Driver's License numbers, the agency intends to reference the Department of Motor Vehicle (DMV) Fraud Hotline in the notice; the agency should seek DMV's approval and provide DMV with advanced warning that DMV may experience a surge of inquiries. Note: This Fraud Hotline is only used when an individual has evidence to suggest their Driver's License number has been misused.

H. Method(s) of Notification

The best means for providing notification will depend on the nature and availability of contact information of the affected individuals, as well as the number of individuals affected. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following are examples of the types of notification which may be considered.

1. First-Class Mail. Written notice to the named individual, whenever possible by first-class mail to the last known address in the agency's records, should be the primary means of notification. For example, the notice should be addressed to "Jane Doe", and in cases of minor children the notice should be addressed "To the Parent of: Jane Doe". Where there is reason to believe the address is no longer current, an agency should take reasonable steps to update the address by consulting with other agencies, such as the U.S. Postal Service (USPS). The USPS will forward mail to a new address, or will provide an updated address via established processes. The notice should also be sent separately from any other mailing so that it stands out to the recipient, and it should be labeled to alert the recipient to the importance of its contents, (e.g., "Important Information Enclosed"), and as to reduce the possibility that it may be mistaken as advertising mail.

   Notification should include sender or return address information unless there are special circumstances which necessitate not doing so. For example, the inclusion of the healthcare office or clinic name or return address may be more harmful than helpful, and further reveal personal information.

2. Telephone. Notification by telephone may be appropriate as a supplement to written notice in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Persons making the notification by telephone should only do so by personal contact with the affected individual, never through a message on answering machine or other parties. In all cases, written notice by first-class mail must be made concurrently.

3. E-Mail. E-mail may only be used to make notification if the notice triggering data elements involved are **limited** to an individual's user name or e-mail address in combination with a password or security question and answer that would permit access to the online account and as consistent with the Federal Electronic Signatures Act (15 U.S. Code 7001). The Federal Electronic Signatures Act requires, among other things, that an agency must have received express consent from the individual to use e-mail as the primary means of communication before making the breach notification. In such cases the agency may provide the security breach notification by e-mail or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account and all other online accounts for which the person uses the same user name or e-mail address and password or security question or answer. Agencies/state entities must keep in mind that notification by e-mail may be problematic because individuals change their e-mail address and often do not notify all parties of the change, and it may be difficult for individuals to distinguish the agency's e-mail notice from a "phishing" e-mail.

4. Substitute Notification. Subdivision (j), (3) of Civil Code Section 1798.29, provides for substitute notification when an agency can demonstrate that more than 500,000 individuals were affected, or the cost of providing notification would exceed $250,000, or the agency does not have adequate contact information on those affected. In accordance with that provision of law, substitute notification consists of **all of the following methods**:

   a. Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Web site, if the agency maintains a Web site. This includes providing a link to the notice on the home page, or first significant page after entering the website. This link shall be displayed in a larger or contrasting text than the surrounding text in order to draw attention to the link.
   b. Notification to major statewide media and to the California Information Security Office within the Department of Technology; and
   c. E-mail notification when the agency has an e-mail address for the individuals. Here, because an agency is also doing a. and b., the e-mail notice **does not** need to meet the requirements of the Federal Electronic Signature Act.

   The posting should also include a link to Frequently Asked Questions (FAQs) and other talking points to assist the public's understanding of the breach and notification process. See the Security Breach FAQ's provided on the Office of the Attorney General's website.

   Further, when making a substitute notification, the public media should be notified as soon as possible after the discovery of the breach because delayed notification may erode public trust. However, an agency's decision to notify the public media in conjunction with substitute notification, or in other situations, will require careful planning and execution so that the agency is adequately prepared to handle follow-on inquiries.

I. Preparation for Follow-on Inquiries from Noticed Individuals

Those affected by the breach can experience considerable frustration if, in the wake of the individual notification or the initial public announcement, they are unable to find sources of additional accurate information. This applies to both follow-on inquiries made to the agency that experienced the breach, as well as to counterpart entities that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, depending upon the nature of the incident and the information involved, certain entities, such as the credit-reporting agencies, may also need to prepare for a surge in inquiries that might far exceed normal workloads (e.g., requests for copies of credit reports and posting of fraud alerts).

Consequently, and as appropriate, agencies/state entities must adequately prepare for follow-on inquiries and must address inquiries in the most efficient and accurate manner possible. In doing so, an agency should consider provisioning for the following:

1. Instructions to each of its public inquiry intake units about where they should direct both telephone and in-person inquiries about the breach from affected individuals, the media, and the public.

2. A toll-free phone line, answered by personnel specifically trained to handle inquiries from affected individuals and the public, especially when the breach has affected a large number of individuals.

3. A complaint resolution and/or escalation process. For example, individuals may be directed to the agency's Office of Civil Rights, if one is available.

4. Early warning and information about the timing of notification to all counterpart entities, so that they may adequately prepare for any potential surge in inquiries.

5. The timing for delivery of the notice to noticed individuals in conjunction with the availability of staff to respond to follow-on inquiries must also be considered. For example, an agency should not release a notification so that it is likely to be received on the last work day before major holiday weekend or the day of an observed holiday.

The OIS can assist agencies/state entities with the development of scripts, FAQs, staff training and other related notification activities.

J. Other Situations When Breach Notification Should Be Considered

Neither state law nor state policy requires notification in the case of breaches involving non-notice-triggering personal information. Nevertheless, breaches involving certain types of non-notice triggering personal information can also implicate a broad range of harms to individuals. The other types of harm that an agency should consider, depending upon the nature of the personal information involved, and the circumstances of the loss or theft, include but are not limited to, the following:

- Harm to reputation.
- Potential for harassment.
- Potential for prejudice, particularly when health or financial benefits information is involved.

- Other types of financial loss, such as an increase or denial of insurance premiums which may be associated with the latter.
- Embarrassment.
- Legal problems.

In situations where other (non-notice-triggering) personal information is involved, an agency should, in consultation with its legal counsel and the OIS, consider the following factors when making an assessment of the likely risks of harm and the decision to notify:

1. Nature of the Data Elements Breached. The nature of the compromised data elements is a key factor to consider in determining if notification should be provided to affected individuals. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive in another context. For example, the breach of a list containing the names and home addresses of undercover peace officers or domestic violence victims, poses a higher risk of harm than a list containing the names of individuals that subscribe to an agency's monthly newsletter on general family issues. Yet in the context of this subscriber list, if the newsletter were specific to a certain profession or clientele it could pose a higher level of risk, such as a newsletter that is specific to a support group for battered persons. It is also important to note that a Social Security number alone is useful in committing identity theft. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of possible harms that could result from their acquisition by or disclosure to unauthorized individuals.

2. Likelihood the Information Is Accessible and Usable. Upon learning of a breach, agencies/state entities should assess the likelihood that personal information will be or has been acquired and misused by unauthorized individuals. An increased risk that the information will be misused by unauthorized individuals should influence the agency's decision to provide notification.

   The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals; however, depending upon any number of physical, technological, and procedural safeguards employed by the agency, the risk of compromise may be low to non-existent. For example, exposure on a public website for many weeks or months would increase the likelihood that it was acquired by an unauthorized individual. Also if the information was properly protected by encryption then the likelihood the information is accessible and usable is non-existent; whereas, "paper copies" of printed personal information are essentially unprotected and would be considered a much higher risk of compromise depending upon the type of information involved.

   In this context, the encryption product and algorithm used has been validated by the National Institute of Standards and Technology (NIST) to the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS), as state agencies are required to use the ANSI and FIPS standards in their information management planning and operations (SAM section 5100).

3. Likelihood the Breach May Lead to Harm. The IPA (Civil Code Section 1798.21) requires agencies to protect against anticipated threats or hazards to the security or integrity of records containing personal information which could result in any injury to individuals. When considering injury to individuals, agencies should consider the broad reach of potential harm and the likelihood harm will occur.

   a. *Broad Reach of Potential Harm.* The number of possible harms associated with the loss or compromise of information may include, but are not necessarily limited to, the following:

      i. the effect of a breach of confidentiality or fiduciary responsibility;
      ii. The disclosure of address information for victims of stalking or abuse, or persons in certain high risk professions (e.g., law enforcement officers, reproductive health care clinic workers, etc.);
      iii. legal problems (e.g., an individual uses another individual's name and Driver's License number when arrested, or a pregnant woman uses the medical identity of a mother and delivers a baby who tested positive for illegal drugs. Consequently, Social Services takes her children from her and she must hire an attorney to prove that she is the victim of medical identity theft);
      iv. harm to reputation;
      v. financial loss;
      vi. the disclosure of private facts and unwarranted exposure leading to embarrassment, humiliation, mental pain, emotional distress, or loss of self-esteem; the potential for secondary uses of the information which could result in fear or uncertainty; or
      vii. the potential for harassment, blackmail, or prejudice, particularly when health or financial benefits information is involved.

   b. *Likelihood Harm Will Occur*. The likelihood that a breach of non-notice triggering personal information may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. While not considered notice-triggering under the law, a Social Security number alone is useful in committing identity theft, and if there is evidence that this information was the specific target of attack by a known identity theft fraud ring, the likelihood of harm would be considered greater than if this same information had been inadvertently exposed or acquired.

4. Ability of the Agency to Mitigate the Risk of Harm to Individuals. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) and/or information affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

   The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the compromised information is a factor in determining the risk of harm, particularly the harms associated with identity theft. Such mitigation may not prevent the use of personal information for identity theft, but it can limit the associated harm.

Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

Where practical, the agency should exhaust its ability to mitigate any risk of harm, and provide timely instruction and guidance in the notice to affected individuals about steps they can take to protect themselves.

5. Ability of the Notified Individuals to Mitigate the Risk of Harm to Themselves. Notification should be designed to afford affected individuals an opportunity to mitigate their risk. For example, in the case where the name and home address of a victim of abuse has been compromised, the individual may, in order to mitigate their risk, choose to move or to affect a greater situational awareness.

   In some cases the apology and assurance of corrective action, addressed through notification, may serve as a satisfactory remedy for those individuals who have been impacted, or potentially impacted, by the breach.

   On the other hand, agencies/state entities should bear in mind that notification, when there is little or no risk of harm might create unnecessary concern and confusion.

   Additionally, under circumstances where notification could increase the risk of harm, the prudent course of action is not to notify.

K. Other Actions That Agencies/State Entities Can Take to Mitigate Harm to Individuals

In addition to notifying affected individuals, it may be necessary for an agency to take other actions to mitigate the risk of harm. For example, if the breach involves government credit cards, the agency should notify the issuing bank promptly; or, if the breach is likely to lead to benefit fraud (e.g., Medi-Cal, Unemployment Insurance, etc.), the agency should notify the benefit agency, so that they can take appropriate actions, such as flagging accounts associated with the affected individuals.

VI. OTHER CONSIDERATIONS

Outside of the legal and policy requirements discussed earlier there are two other steps an agency may consider to mitigate the effects of a breach on the agency and the individuals. The first is advanced notification to the media and the second is credit monitoring services. These are discussed in more detail below.

A. Advance Notification to the Media

Though not required, in breaches likely to receive greater attention, an agency may consider providing advance notification to the media as notifications are mailed to individuals. This allows the agency to present the facts of the story first, rather than trying to correct inaccurate or incomplete news stories after they are published. Advance notification to the media also demonstrates openness and can promote good ongoing communications with reporters. In addition, providing accurate information through the news media is another way to reach those affected and to explain what steps they can take to protect themselves.

As mentioned above, the timing of any notification to media or individuals is critical. The agency must ensure it is prepared to handle follow-on inquiries and is appropriate given the circumstances. In some cases, it may be more prudent not to notify news media at the same time notification is made to affected individuals. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains, and may wipe the laptop clean before selling it. In such a case, public announcement may actually alert a thief to what he possesses, increasing the risk that the information will be misused, and it would be wise to delay media notification at least until affected individuals have received notice and had time to take defensive action.

B. Credit Monitoring Services

The offer of credit monitoring services can provide an additional measure of protection for individuals affected by a breach - especially where the compromised information presents a risk of new accounts being opened. However, this involves agency expense and the services are only useful in cases where there has been a breach of Social Security number, California Driver's License, or California Identification Card number. Credit monitoring is not helpful for breaches of account numbers only. When a "free" mitigation product is offered, be sure that the individuals are not automatically enrolled for a renewal at their own cost.

Credit monitoring is a commercial service that cannot prevent or guarantee that identity theft will not occur; however, it can assist individuals in early detection of instances of new-account identity theft, thereby allowing them to take steps to minimize the harm. Typically, the service notifies individuals of activities on their credit files, such as creation of a new account or inquiries to the file. Consult the Consumer Federation of America consumer resource publications "Best Practices for Identity Theft Services" and "Best Practices for Identity Theft Services: How Are Services Measuring Up?".

VII. NOTIFYING OTHERS WHEN REQUIRED

A. Notifying the Attorney General

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. [Civil Code section 1798.29 (a) and Civil Code Section 1798.82 (a)].

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. [Civil Code Section 1798.29(e) and Civil Code section 1798.82(f)]

Use the Attorney General's online form to submit a sample of the security breach notification at: http://oag.ca.gov/ecrime/databreach/reporting.

B. Notifying Credit Reporting Agencies

Sending breach notification letters involving a breach of Social Security numbers or Driver's License/California ID numbers can result in a large volume of calls to consumer credit reporting agencies, affecting their ability to respond efficiently. Be sure to contact these agencies before you send out notices in cases involving a large number of individuals - 10,000 or more. Note that this step is not relevant for breaches of a single account number or of medical or health insurance information alone. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason. You may contact the credit reporting agencies as follows:

- Experian: Send an e-mail to BusinessRecordsVictimAssistance@Experian.com.
- Equifax: Send an e-mail to businessrecordsecurity@equifax.com.
- TransUnion: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

VIII. APPENDICES

To assist the agency with responding to a breach and drafting a breach notice the following breach response checklist, and the sample breach notices and the corresponding document enclosure has been provided as appendices herein.

Note: If a breach involves more than one type of notice-triggering information, the notice should use language from all the relevant sample notices. Further, when deceased person's or minor children's personal information is involved, special content and recommended actions are necessary for inclusion in the notification. Consult OIS in these cases.

Appendix A: Breach Response and Notification Assessment Checklist

Appendix B: Sample Breach Notice - Social Security Number

Appendix C: Sample Breach Notice - Driver's License or California ID Card Number

Appendix D: Sample Breach Notice - Credit Card or Financial Account Number

Appendix E: Sample Breach Notice - Medical Information

Appendix F: Sample Breach Notice - Health Insurance Information

Appendix G: Sample Breach Notice - Hybrid

Appendix H: Sample Breach Notice – Automated License Plate Recognition System

Appendix I: Sample Breach Notice – User Name or E-mail Address

Appendix J: Breach Help –Consumer Tips Enclosure (English)

Appendix K: Breach Help –Consumer Tips Enclosure (Spanish)

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
1. Assemble State Entity Response Team	p. 5			
1.1. Escalation Manager/Team Lead	p. 5			
1.2. Program Manager (office experiencing the breach)	p. 5			
1.3. Information Security Officer	p. 5			
1.4. Chief Privacy Officer or Coordinator	p. 5			
1.5. Public Information Officer or Communications Officer	p. 5			
1.6. Legal Counsel	p. 5			
1.7. Other	p. 5			
1.8. Chief Information Officer or Technology Specialist	p. 5			
1.9. Personnel Office or Human Resources Manager	p. 5			
2. Escalation/Internal Reporting	p. 5			
2.1. Deputy Director	p. 5			
2.2. Director	p. 5			
2.3. Agency Secretary	p. 5			
2.4. Governor's Office	p. 5			
3. Is an impact assessment/coordination meeting necessary?	p. 5			
3.1. Agency Response Team Members to Attend	p. 5			
3.2. OIS Response Team Member to Attend	p. 5			
3.3. CCIU Response Team Members to Attend	p. 5			
3.4. Sign in Sheet / Attendee roster needed	p. 5			
3.5. Non-disclosure agreement forms needed	p. 5			
4. Security Incident Reporting	p. 5			
4.1. Reported through Cal-CSIRS	p. 5			
4.2. Respond to CHP CCIU response inquiry	p. 5			
4.3. Respond to OIS response inquiry	p. 5			
4.4. Update follow-up report (SIMM 5340-B) through Cal-CSIRS	p.6			
5. Is breach notification required by law (Civil Code Section 1798.29)?	p. 7			
5.1. Was computerized data owned or licensed by the agency involved?	p. 7			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.2. Was a computer system, equipment, or peripheral storage device (capable of containing computer data) involved?	p. 7			
5.3. Were notice-triggering data elements involved?				
5.3.1. First name or first initial and last name, and one or more of the following:	p. 7			
5.3.2. Social Security number.	p. 7			
5.3.3. Driver's License number or California Identification Card	p. 7			
5.3.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 7			
5.3.5. Medical information (as defined in Civil Code Section 1798.29).	p. 7			
5.3.6. Health insurance information (as defined in Civil Code Section 1798.29).	p. 7			
5.3.7 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 7			
5.3.8 A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 8			
5.4. Were the notice-triggering data elements encrypted?	p. 8			
5.4.1. Was the encryption product used, a FIPS -140 validated or NIST certified cryptographic module?	p. 8			
5.5. Were notice triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person? ***(Examples only-list is not limited to these***):	p. 8			
5.5.1. The system, equipment, or information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information.	p. 8			
5.5.2. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred).	p. 8			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
5.5.3. The attacker deleted security logs or otherwise "covered their tracks".	p. 8			
5.5.4. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting.	p. 8			
5.5.5. The attack vector used is known to seek and collect personal information.	p. 8			
5.5.6. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.	p. 8			
6. Is breach notification required by Information Technology policy	p. 9			
6.1. Was data, of any media type or format (e.g., paper, cassette tape), owned or licensed by the agency involved?	p. 9			
6.2. Were notice-triggering data elements involved?	p. 9			
6.2.1. First name or first initial and last name, and one or more of the following:	p. 9			
6.2.2. Social Security number.	p. 9			
6.2.3. California Driver's License or Identification Card number.	p. 9			
6.2.4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	p. 9			
6.2.5. Medical information (as defined in Civil Code Section 1798.29)	p. 9			
6.2.6. Health insurance information (as defined in Civil Code Section 1798.29)	p. 9			
6.2.7 Automated License Plate Recognition (ALPR) System information (as defined in Civil Code Section 1798.90.5).	p. 9			
6.2.8 A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.	p. 9			
6.3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired? ***(Examples only-list is not limited to these)***:	p.9			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
6.3.1. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information.	p.9			
6.3.2. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.	p.10			
6.3.3. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported or fraudulent accounts opened.	p.10			
7. Timeliness of Notification	p.10			
7.1. Notification can be sent within ten (10) days from the date data acquisition has been determined.	p.10			
7.2. Notification may be delayed due to legitimate needs of law enforcement.	p.10			
7.3. Notification may be delayed to determine scope of breach.	p.10			
7.4. Notification may be delayed to restore system to reasonable integrity.	p.10			
7.5. Delay will or may exacerbate the risk of harm to individuals.	p.10			
7.6. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) has authorized the delay of notification.	p.10			
8. Source of Notification	p. 10			
8.1. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) will sign the notice.	p. 10			
8.2. The notice is addressed by the entity in which the recipient has a relationship.	p. 10			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
8.3. The notice is addressed by an entity in which the recipient has no direct relationship, but the relationship is explained sufficiently in the notice.	p. 10			
9. Format of Notice	p. 11			
9.1. The notice shall be designed to call attention to the nature and significance of the information it contains, and shall be formatted on official	p. 11			
9.1.1. No smaller than 10-point Ariel font type;	p. 11			
9.1.2. A title "Notice of Data Breach"; and	p. 11			
9.1.3. Contain at a minimum the following headings: • "What Happened"; • What Information Was Involved"; • "What We Are Doing"; • "What You Can Do"; • "Other Important Information"; and • "For More Information ".	p. 11			
10. Content of Notice	p. 11			
10.1. The notice leverages the sample notifications provided by OIS.	Appendices B-I			
10.2. The notice is clear and concise.	p. 11			
10.3. The notice uses easy-to-understand language and does not include technical jargon.	p. 11			
10.4. The notice includes a general description of what happened; including the date of breach if known, or estimated date or date range within which the breach occurred.	p. 11			
10.5. The notice specifically identifies the data elements involved.	p. 11			
10.6. The notice includes the steps the individual can/should take to protect themselves from harm (if any).	p. 12			
10.7. The notice includes an apology.	p. 12			
10.8. The notice includes information about what the agency has done or is doing to investigate the breach, mitigate the losses, and protect against any further breaches.	p. 12			
10.9. The notice includes the name and contact information of an individual contact(s) at the agency with the ability to provide more information about the breach to the	p. 12			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
10.10. The notice provides a toll-free number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free number a local number for the contact is provided.	p. 12			
10.11. The agency has knowledge that affected individuals are not English speaking and has prepared notices in the appropriate languages.	p. 12			
10.12. The agency has given consideration in providing the notification to individuals who are visually or hearing impaired (e.g., establishing a TDD or posting a large-type notice).	p. 12			
11. Approval of the Notice	p. 12			
11.1. Draft notice submitted to OIS for review and approval prior to their release:	p. 12			
11.1.1. Communicated with an OIS security representative by telephone contact, prior to submission.	p. 12			
11.1.2. Submitted breach notification into Cal-CSIRS, selecting "Breach Notification for Review" as the type.	p. 12			
11.1.3. Have allowed at least one full business day for OIS review.	p. 12			
11.2. Final notice submitted to OIS and includes required information.	p. 13			
11.3. The agency has notified and/or sought prior approval for release of notice or the use of reference from other public and private sector agencies that may be impacted by the breach or play a role in mitigating the potential harms (e.g., credit reporting agencies, etc.).	p. 13			
12. Method of Notification	p. 13			
12.1. First-class mail notification will be made.	p. 13			
12.1.1. Addressed to the named individual.	p. 13			
12.1.2. Mailed to the last known address.	p. 13			
12.1.3. Mailed separately from other letters and notices.	p. 13			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
12.1.4. Labeled on the outside of the envelope to alert recipient to the importance of its contents (e.g., "Important Information Enclosed") as to reduce the likelihood it is mistaken for	p. 13			
12.1.5. Includes sender or return address information. Special caveats noted here.	p. 13			
12.2. Telephone notification will be made with a concurrent follow-up written by first-class mail.	p. 14			
12.3. E-mail notification will be made as the following criteria are met:	p.14			
12.3.1. Individual has provided agency with an e-mail address.	p.14			
12.3.2. Individual has provided written consent to use e-mail as the primary means of communication.	p.14			
12.3.4. E-mail notification is consistent with the provisions regarding electronic records and signatures set forth in the Federal Electronics Signatures Act (15 U.S. Code 7001).	p.14			
12.4. Substitute notification will be made as the following criteria are met:	p. 14			
12.4.1. Agency has demonstrated that more than 500,000 individuals were affected; or the cost of providing notification would exceed $250,000; or the agency does not have adequate contact information on those affected (no known mailing address is available).	p. 14			
12.4.2. Substitute notification, as required, will include the following collectively: 1) Conspicuous posting on the agency website; 2) Notification to statewide media; and 3) E-mail notification when the agency has an e-mail address to individuals. Here, the requirements of the Federal Electronics Signatures Act **do not** need to be met.	p 14			
12.4.3. Web posting will be made on homepage or a conspicuous link from the homepage.	p.14			

12.4.4. Web posting will also include a link to FAQs.	p.14			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
12.4.5. Information in press release will not impede or compromise the investigation or pose other security risks.	p.15			
12.5. Agency has elected to issue press release, as well as first-class notification due to the number of individuals affected.	p.15			
12.5.1. Information in press release will not impede or compromise the investigation or pose other security risks.	p.15			
13. Preparation for Follow-on Inquiries from Noticed Individuals	p.15			
13.1. The agency's public intake areas have been alerted and trained as appropriate to properly direct telephone and in-person inquiries about the breach.	p.15			
13.1.1. Inquiries from the press are to be directed to:	p. 15			
13.1.2. Inquiries from individuals receiving the notice and needing more information are directed to:	p. 15			
13.2. The agency has provisioned for a toll-free call center, staffed with trained personnel.	p. 15			
13.3. The agency has provisioned for documented scripts, and answers to anticipated and frequently asked questions.	p. 15			
13.4. The agency has provisioned for a complaint resolution and/or escalation process.	p. 15			
13.5. The agency has provided early warning and information about the timing of notification to all counterparts, so that they are prepared for the potential surge in inquiries (e.g., credit reporting agencies, etc.).	p. 15			
14. Other Situations When Breach Notification Should be Considered	p. 16			
14.1. The agency has considered the nature of any non-notice triggering personal information involved in this breach and the potential harms it poses or may pose to affected individuals.	p. 16			
14.1.1 The agency has determined the nature of the information does potentially pose one or more of the following potential harms ***(Examples only-list is not limited to these***):	p. 16			
14.1.1.1. Harm to reputation.	p. 16			

14.1.1.2. Potential for harassment.	p. 16			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
14.1.1.3. Potential for prejudice, particularly when health or financial benefits information is involved.	p. 16			
14.1.1.4. Financial loss.	p. 16			
14.1.1.5. Embarrassment.	p. 16			
14.1.1.6 Legal problems.	p. 16-18			
14.2. The agency has considered the likelihood that the information has been acquired, or is accessible and usable.	p. 16			
14.2.1. The agency has determined it is known or highly likely the information has been acquired and has the potential for misuse by unauthorized persons due to the following ***(examples only-list is not limited to these***):	p. 16			
14.2.1.1. The information was not encrypted.	p. 16			
14.3.1.2. The list was posted on the Internet for an extended period of time.	p. 16			
14.2.1.3. The encryption product used was not a NIST certified cryptographic module or FIPS-142 validated product.	p. 17			
14.3. The agency determined there is a likelihood that the breach may lead to harm due to the following ***(examples only-list is not limited to these***):	p. 17			
14.3.1. breach of confidentiality or fiduciary responsibility;	p. 17			
14.3.2. disclosure of address for victims of stalking or abuse; or persons in high risk professions;	p. 17			
14.3.3. legal problems;	p. 17			
14.3.4. harm to reputation;	p. 17			
14.3.5. financial loss;	p. 17			
14.3.6. disclosure of private facts and unwanted exposure; potential for secondary uses of the information which could result in fear or uncertainty;	p. 17			
14.3.7. potential for harassment, blackmail, or prejudice;	p. 17			
14.3.8. the social security number alone can lead to identity theft.	p. 17			
14.4. The ability of the agency to mitigate the risk of harm to individuals.	p.17			

14.4.1. The agency can mitigate further compromise of the system.	p.17			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 5340-C Reference	Yes	No	Notes/Comments
14.4.2. The agency can monitor systems for misuse of the personal information and patterns of suspicious behavior.	p.17			
14.4.3. The agency has exhausted its ability to mitigate any further risk of harm.	p.18			
14.4.4. The apology and assurance of corrective action may serve as a satisfactory remedy those impacted.	p.18			
14.5. The ability of the noticed individual to mitigate the risk to themselves following notification.	p.18			
15. Other Actions Agencies Can Take to Mitigate Harm	p.18			
15.1. The agency has notified financial institutions if state payroll or bank account information was involved.	p.18			
15.2. The agency has notified other agencies about the potential for benefit fraud as applicable (e.g., disability, unemployment, Medi-Cal,	p.18			
16. Other Considerations When State Employee Data Is Involved				
16.1. Agency has treated affected employees with the same care and concern as any other individual affected by breach.	p.18			
16.2. Agency has considered other early warning and notification methods to augment the first-class mail notification (e.g., such as e-mail, Intranet posting, town hall meetings).	p.18			
16.3. Agency has notified managers and supervisors of the affected employees and adequately prepared them to answer questions from employees.	p.18			
16.4. Agency has considered notifying represented employee organizations as may be appropriate.	p.18			
16.5. Agency has considered the use of town hall meetings to respond to employee questions and concerns following notification.	p.18			
17. Other Considerations From a Public Relations Perspective	p. 18			
17.1. The agency has considered advanced notification to the media.	p. 18			

17.2. The agency has considered acquiring credit monitoring services for the affected individuals. Note: This should only be considered when the incident involves Social Security number	p. 19			
18. Notifying Others When Required	p. 19			
18.1. Notifying the California Attorney General and uploading a redacted copy of the notification to their website when the incident requires notification to 500 or more individuals.	p. 19			
18.2. Notifying the Credit Reporting Agencies when notification is made to 10,000 or more individuals.	p. 20			

APPENDIX B: Sample Breach Notice: Social Security Number

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your social security number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure " Breach Help –Consumer Tips from the California Attorney General ".
Other Important Information:	Enclosure " Breach Help –Consumer Tips from the California Attorney General "
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

_____ _____

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX C: Sample Breach Notice: Driver's License or California ID Card Number

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your driver's license number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure " Breach Help –Consumer Tips from the California Attorney General ".
Other Important Information:	Enclosure " Breach Help –Consumer Tips from the California Attorney General "
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX D: Sample Breach Notice: Credit Card or Financial Account Number

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your first and last name, along with your bank account number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	To help prevent unauthorized access and fraudulent activity on this account, we recommend that you immediately contact [the credit card or financial account issuer] and close your account. Tell them that your account may have been compromised, and ask that they report it as "closed at customer request." If you want to open a new account, ask your account issuer to give you a PIN or password associated with the new account. This will help control access to the account.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
For More Information:	For more information on identity theft, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX E: Sample Breach Notice: Medical Information Only

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your medical information [*or medical history, medical condition, or medical treatment or diagnosis*] was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [provider or plan], to serve as a baseline.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General"
For More Information:	For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

_____
[*Signature of State Entity Head or Delegate*] [*Title*]

[1] **Additional language will be necessary if other notice triggering information was involved. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so and refer to the following language.**

APPENDIX F: Sample Breach Notice: Health Insurance Information Only

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*][1] Please note, the information was limited to [*specify, (e.g., your name and health plan number*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your health insurance information [*or policy, plan number, or subscriber identification number*] was involved.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. We also recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.
Other Important Information:	Enclosure " Breach Help –Consumer Tips from the California Attorney General "
For More Information:	For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

[1] **Additional language will be necessary if other notice triggering information was involved. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so and refer to the following language.**

APPENDIX G: Sample Breach Notice: Hybrid (SSN and Health Information)

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*]. An employee inadvertently e-mailed a document containing your personal information to the wrong person.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] The document contained your [*specify, (e.g., your name and health plan number)*] along with your social security number.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence.
What You Can Do:	Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. Because your Social Security number was involved, in order to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure. Since your health insurance information was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*name of health insurance provider*]. If you see any service that you believe you did not receive, please contact us at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.
Other Important Information:	Enclosure " Breach Help –Consumer Tips from the California Attorney General "
For More Information:	For more information about privacy protection steps and your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX H: Sample Breach Notice: Automated License Plate Recognition System

[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at [*XYZ Solutions, Inc.*]. XYZ Solutions, Inc. is an Automated License Plate Recognition (ALPR) system operator and maintains an ALPR system database used by many state and local law enforcement entities, including ours, to administer public safety and crime protection programs. We received notification on [*date notification received*] that an XYZ Solutions ALPR system database has been compromised.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*] Please note, the information involved was limited to your name, address, vehicle license plate number, and the vehicle's location and patterns of movement, if any, between [*month day, year and month day, year*]. This incident did not involve any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that the incident is being investigated to determine and correct the cause, and to minimize the risk of recurrence.
What You Can Do:	Your privacy is of utmost concern to us. For more information about your privacy rights, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX I: Sample Breach Notice: User Name or E-Mail Address
[Agency Letterhead]

[Date]

[Addressee]
[Mailing Address]
[City] [State] [Zip Code]

[Salutation]

Subject: NOTICE OF DATA BREACH

What Happened?	[*Describe what happened in general terms, see example below*] We are writing to you because of a recent security incident that occurred on [*date of incident]* at *[name of organization*] involving the Online Information Sharing Portal (OISP). Our security systems detected an abnormally large number of attempts to access OISP user accounts. The computer generated password guessing activity was designed to randomly guess user password combinations until account access is ultimately achieved. Further investigation revealed that some user account passwords were successfully guessed before the activity was detected and blocked.
What Information Was Involved?	[*Describe what specific notice-triggering data element(s) were involved, see example below*]. Please note, the information was limited to your user identification (email address), password and security questions for your OISP online account. This incident did not involve the compromise or access to any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. However, if you use the same user identification, password and or security question for any other online accounts those may be at risk.
What We Are Doing:	[*Note apology and describe what steps your agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches, see example below*] We regret that this incident occurred and want to assure you that we have implemented additional security controls to minimize the risk associated with this occurrence and the risk of recurrence. These include prompting all system users to update their profile and reset their passwords and security questions, and implementing automated validation at password creation to ensure the use of unique, hard-to-guess passwords, and established limits on the number of failed attempts to access your account.
What You Can Do:	To protect against unauthorized access and use of your online account(s), we recommend, if you haven't already done so, that you immediately change your password and security questions. Choose a unique, hard-to-guess password for each of your online accounts and always look for and report unusual activity in your accounts. A hard-to-guess password contains at least eight characters and is a combination of upper and lower case letters, numbers and special characters.
Other Important Information:	Enclosure "Breach Help –Consumer Tips from the California Attorney General".
For More Information:	For more information about online protections, you may visit the Web site of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.
Agency Contact:	Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Signature of State Entity Head or Delegate*] [*Title*]

APPENDIX J: Breach Help – Consumer Tips Enclosure (English)

Breach Help

Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

Credit or Debit Card Number

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

Credit Card

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to $50 when you report them, and most banks have a zero-liability policy.[1]

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

Debit Card

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

Office of the Attorney General
California Department of Justice

Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to $50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.[2]

3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

Social Security Number

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see ***How to Freeze Your Credit Files*** at *www.oag.ca.gov/privacy/info-sheets*.

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

Password and User ID

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.

2. If you use the same password for other accounts, change them too.

3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.

4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.

5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.

   Example: "I love tropical sunsets" becomes 1luvtrop1calSuns3ts!

6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation (*www.eff.org*) lists some free versions and computer magazines offer product reviews.

Bank Information

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)

2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

Driver's License Number

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at *dlfraud@dmv.ca.gov*. Do not include personal information on your e-mail.

Medical or Health Insurance Information

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.

2. If the letter says your health insurance or health plan number was involved, contact

your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow up on it with your insurer or plan. For more on medical identity theft, see ***First Aid for Medical Identity Theft: Tips for Consumers***, at *www.oag.ca.gov/privacy/info-sheets*.

For more details on what to do if you suspect that your information is being used to commit identity theft, see the ***Identity Theft Victim Checklist*** at *www.oag.ca.gov/idtheft/information-sheets.*

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

NOTES

[1] Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

[2] Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.

APPENDIX K: Breach Help – Consumer Tips Enclosure (Spanish)

Ayuda en caso de robo de datos confidenciales

Consejos para el consumidor del Procurador General de California

Hoja 17 de información al consumidor • Octubre de 2014

Suponga que recibe una carta de una compañía, agencia del gobierno, una universidad, un hospital u otra organización, La carta dice que su información personal puede haber formado parte de un robo de datos confidenciales. O quizás se entere del episodio por un boletín de noticias o sitio web de la empresa. Cualquiera sea la manera en que reciba la información, el hecho de que se haya violado la seguridad de los datos de una compañía no quiere decir que usted haya caído víctima de robo de identidad o sufrido un daño, pero existe el riesgo de que así sea.

El aviso de violación de datos confidenciales debería indicar los tipos específicos de información personal involucrados. También le puede decir lo que la organización está haciendo para contrarrestar el problema. Para protegerse a sí mismo, puede tomar los pasos que se indican a continuación. Todo dependerá del tipo de información personal afectada en el robo de los datos confidenciales.

Algunas compañías afectadas le ofrecerán sin cargo una alerta de crédito, lo cual le alerta después de que alguien solicitó u obtuvo un crédito nuevo en su nombre. La alerta de crédito puede ser útil cuando le roban su número del Seguro Social. Pero no le avisa cuando se produce actividad fraudulenta en su cuenta existente de tarjeta de crédito o débito.

Número de tarjeta de crédito o débito

El aviso de robo de datos confidenciales quizás le informe cuándo y dónde se produjo dicha violación. Si usó su tarjeta de crédito o débito en ese lugar en el periodo indicado, puede tomar pasos para protegerse.

Tarjeta de crédito

1. Vigile su cuenta de tarjeta de crédito para ver si hay transacciones sospechosas, y denúncielas al banco que emitió la misma (o a American Express o Discover). Pídale al banco que habilite la vigilancia y alertas en línea para esa cuenta. De esa manera podrá recibir un aviso anticipado de cualquier transacción fraudulenta.

2. Si observa transacciones fraudulentas en su tarjeta de crédito después de haberse anunciado el robo de datos confidenciales, considere la posibilidad de cancelar su tarjeta de crédito. Puede disputar las transacciones fraudulentas que aparezcan en su estado de cuenta, y deducirlas del monto adeudado. Su responsabilidad por transacciones fraudulentas se limita a $50 cuando las denuncia, y la mayoría de los bancos tienen políticas que lo eximen a usted de toda responsabilidad.[1]

Office of the Attorney General
California Department of Justice

Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

3. Si cancela su tarjeta de crédito, no se olvide de comunicarse con todas las compañías que deducen sus pagos de la tarjeta en forma automática. Si quiere seguir haciendo pagos en forma automática, deles su nuevo número de cuenta.

Tarjeta de débito

1. Vigile su cuenta de tarjeta de débito para ver si hay transacciones sospechosas, y denúncielas a su banco. Pídale al banco que habilite la vigilancia y alertas en línea para esa cuenta. De esa manera podrá recibir un aviso anticipado de cualquier transacción fraudulenta.

2. Denuncie toda transacción no autorizada a su banco inmediatamente para evitar responsabilidad. Su responsabilidad por transacciones fraudulentas se limita a $50 si las reporta en un plazo de dos días. Su banco puede tener llegar a eximirlo de toda responsabilidad. Pero si deja pasar el tiempo, su responsabilidad aumentará, hasta llegar al monto total de la transacción si no la reporta en un plazo de 60 días de su aparición en su estado de cuenta.[2]

3. Considere la posibilidad de cancelar su tarjeta de débito. Esta tarjeta está conectada con su cuenta bancaria. La manera más segura de protegerse contra la posibilidad de que le saquen dinero de su cuenta bancaria con un número robado es cancelar la tarjeta. Si bien es probable que le devuelvan el dinero robado, es posible que esto no ocurra hasta que su banco haya completado su investigación.

Número del Seguro Social

Si el aviso le dice que quizás le han robado su número del Seguro Social, tiene que hacer lo siguiente.

1. Comuníquese con las tres agencias de información de crédito. Puede denunciar un robo potencial de identidad a las tres agencias principales de información de crédito llamando a cualquiera de los números gratis para denunciar fraude que aparecen a continuación. Lo atenderá un sistema telefónico automatizado que le permitirá marcar su expediente con un alerta de fraude en las tres agencias de información de crédito. También le enviarán instrucciones sobre cómo obtener una copia de su informe de cada una de las agencias de información de crédito.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. Qué significa poner una alerta de fraude en su expediente de crédito. Una alerta de fraude ayuda a protegerlo contra la posibilidad de que un ladrón de identidad abra una cuenta de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de alguien que está solicitando una cuenta de crédito, recibirá un aviso de que puede haber fraude en la cuenta. Esto alertará al comerciante para que tome los pasos necesarios para verificar la identidad del solicitante. Un alerta de fraude dura 90 días y se puede renovar. Para obtener información sobre un nivel de protección aún mayor, lea ***How to Freeze Your Credit Files*** *(Cómo congelar sus datos de crédito)* en *www.oag.ca.gov/privacy/info-sheets.*

3. Revise sus informes de crédito. Examine cada uno de ellos cuidadosamente. Fíjese si hay alguna cuenta que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas *(inquiries)* para ver si hay nombres de acreedores a quienes usted no les solicitó crédito. Algunas compañías facturan con nombres distintos

que el de su tienda. La agencia de información de crédito le podrá decir cuando éste sea el caso. Algunas consultas pueden ser identificadas como "promocionales". Estas son cuando una empresa le ha pedido a una agencia de información de crédito su nombre y dirección para enviarle una oferta de crédito. Las consultas promocionales no son señales de fraude. (Cuando coloque una alerta de fraude, lo borrarán automáticamente de las listas para recibir ofertas de este tipo que usted no solicitó.) Además, como precaución general, fíjese en la sección sobre información personal para ver si hay alguna dirección donde usted nunca vivió.

4. Si encuentra algo que no comprende en su informe de crédito, llame a la agencia, al número que aparece en el informe. El personal de la agencia de información de crédito repasará el informe con usted. Si la información no se puede explicar, tendrá que llamar a los acreedores correspondientes y denunciar el delito en su comisaría local u oficina del alguacil.

Nombre de usuario y contraseña

En el caso de que la violación de seguridad de los datos involucre la contraseña de su cuenta en línea, quizás reciba un mensaje por correo electrónico o cuando inicie una sesión en la página web de su cuenta. Si se entera que quizás le han robado su nombre de usuario y contraseña, o su dirección de correo electrónico o la respuesta a sus preguntas de seguridad, puede tomar los siguientes pasos.

1. Cambie la contraseña de la cuenta afectada. Si no puede ingresar en su cuenta, comuníquese con el servicio al cliente o departamento de seguridad de la compañía.

2. Si usa la misma contraseña en otras cuentas, cámbielas también.

3. Si le robaron su respuesta a la pregunta de seguridad, cámbiela. No use preguntas de seguridad cuya respuesta se puede obtener por un medio público, como el nombre de soltera de su madre, el nombre de su mascota o el nombre de su escuela.

4. Use contraseñas distintas para cada una de sus cuentas en línea. Esto es particularmente importante para cuentas que tienen información sensible, como sus datos médicos o financieros. Tenga en cuenta, por ejemplo, que algunas de sus cuentas en línea pueden tener almacenado el número de su tarjeta de crédito.

5. Genere contraseñas robustas. Cuanto más largas, mejor. Deberían tener por lo menos diez caracteres, con una mezcla de mayúsculas, minúsculas, números, signos de puntuación y símbolos. No use palabras que se pueden encontrar en el diccionario. Puede basar sus contraseñas en una frase, canción o título de un libro.

   Ejemplo: "Viaje al centro de la Tierra" se puede convertir en V1aj3. al.c3ntr0.d3.la.Ti3rra

6. Un programa de administración de contraseñas o "caja fuerte" de contraseñas puede ayudarle a crear y administrar muchas contraseñas robustas. Estos programas pueden funcionar en su computadora, teléfono u otros dispositivos portátiles. Solo tiene que recordar una contraseña (o frase) para abrir la caja fuerte. La organización Electronic Frontier Foundation *(www.eff.org)* lista algunas versiones gratis, y puede ver análisis de estos productos en las revistas de informática.

Información bancaria

Si el aviso sobre la violación de seguridad datos le informa que quizás le robaron su número de cuenta bancaria, por ejemplo de una copia de su cheque, tome los siguientes pasos.

1. Llame al banco e infórmeles sobre la violación. Dígales que quiere cerrar su cuenta. Averigüe si hay cheques suyos que todavía no se cobraron. Quizás le convenga esperar hasta que se hayan cobrado antes de cerrar la cuenta. (O puede escribirle a cada uno de sus acreedores, informarles sobre la violación de datos, incluir un cheque de su cuenta nueva y pedirles que no cobren el cheque que les envió anteriormente.)

2. Abra una nueva cuenta bancaria. Dígale al banco que quiere usar una nueva contraseña para acceder a su nueva cuenta. No use el nombre de soltera de su madre o las últimas cuatro cifras de su número del Seguro Social. Pídale a su banco que notifique a su compañía de verificación de cheques que la cuenta anterior se ha cerrado.

Número de licencia de manejar

Si el aviso de violación de la seguridad de datos le informa que quizás le hayan robado su número de licencia para manejar o tarjeta de identificación de California, y sospecha que puede haber sido víctima de un robo de identidad, comuníquese con la Unidad de Análisis y Fraude de Licencias de Manejar (DL-FAU, por sus siglas en inglés) del DMV llamando al 1 866-658-5758 o escribiendo a *dlfraud@dmv.ca.gov*. No incluya ninguna información personal si escribe por correo electrónico.

Información de su seguro médico o de salud

Si el aviso le indica que quizás le robaron su número de seguro de salud o plan de salud, tome los siguientes pasos para protegerse contra un posible robo de identidad médica. Una violación de su información médica que no incluya su número del seguro o plan de salud en general no presenta un riesgo de robo de identidad médica.

1. Si la carta dice que quizás le robaron su número del Seguro Social, vea la sección precedente sobre el robo de números de Seguro Social. Comuníquese también con su compañía de seguros o plan de salud, como se indica en el punto 2 a continuación.

2. Si la carta dice que su número de seguro de salud o de plan de salud quedó expuesto, comuníquese con su aseguradora o plan. Cuénteles sobre la violación y pídales que pongan una nota sobre la misma en sus registros y que marquen su número de cuenta.

3. Inspeccione de cerca sus cartas de Explicación de beneficios para ver si hay algún elemento cuestionable. La carta de Explicación de beneficios viene por correo, en general con un aviso que dice "This is not a bill (Esta no es una factura)". Enumera los servicios médicos recibidos por usted y los demás miembros cubiertos por su plan. Si ve un servicio que no recibió, infórmele a su compañía o plan de seguro. Para obtener más información sobre el robo de identidad médica, lea ***First Aid for Medical Identity Theft: Tips for Consumers*** *(Primeros auxilios para el robo de identidad médica: Consejos para consumidores)* en *www.oag.ca.gov/privacy/info-sheets.*

Para obtener más detalles sobre lo que tiene que hacer si sospecha que se está usando su información para cometer robo de identidad, lea ***Identity Theft Victim Checklist*** (*Lo que*

deben hacer las víctimas de robo de identidad) en *www.oag.ca.gov/idtheft/information-sheets.*

Esta hoja se proporciona con fines informativos y no debe interpretarse como asesoramiento legal ni como la política del estado de California. Si desea obtener asesoramiento sobre un caso en particular, debe consultar con un abogado u otro experto. Esta hoja de información se puede copiar, siempre y cuando (1) no se cambie ni se desvirtúe el significado del texto copiado, (2) se dé crédito al Departamento de Justicia de California y (3) todas las copias se distribuyan sin cargo.

Esta hoja se proporciona con fines informativos y no debe interpretarse como asesoramiento legal ni como la política del Estado de California. Si desea obtener asesoramiento sobre un caso en particular, debe consultar con un abogado u otro experto. Esta hoja de información se puede copiar, siempre y cuando (1) no se cambie ni se desvirtúe el significado del texto copiado, (2) se dé crédito al Departamento de Justicia de California y (3) todas las copias se distribuyan sin cargo.

NOTAS

[1] Truth in Lending Act (Ley de Veracidad en los Préstamos), Código de los Estados Unidos, título 14, sección 1601 y subsiguientes.

[2] Electronic Funds Transfer Act (Ley de Transferencia Electrónica de Fondos), Código de los Estados Unidos, título 15, sección 1693 y subsiguientes.

State of California
DEPARTMENT OF COMMUNITY SERVICES AND DEVELOPMENT
CSD 415 (Rev.0 4/17/18)

ECIP/HEAP PAYMENT REQUEST AND CONFIRMATION
(NON-REGULATED UTILITY COMPANIES ONLY)

To:	Utility Company's Name:	Attention:		
From:	Agency's Name:			Date of Request:
	Mailing Address:	City:	State:	Zip:
	Agency Contact Person:		Phone:	

Instructions to non-regulated utility companies:

1. Once a client's account has been credited, enter the date in the "DATE CREDITED" column.
2. After all accounts have been credited, sign and date the form in the space provided below.
3. Return this form to the agency's contact person at the address identified above.

The following utility payments are being made on behalf of these clients:

	Name and Address of Client	Utility Account #	Payment Amount	Date Credited
1.			$	
2.			$	
3.			$	
4.			$	
5.			$	
6.			$	
7.			$	
8.			$	

UTILITY COMPANY CERTIFICATION

I hereby certify that the referenced accounts were credited in the amounts shown.

Name/Title	Signature of Approval	Date

AGENCY USE ONLY

Total Payments	$	Check Number	#

ECIP/HEAP PAYMENT REQUEST AND CONFIRMATION
CSD 415 (Rev. 04/17/18)
Instructions

This form will be used by the agency and non-regulated utility company in compliance with Section 2605(b)(7), item (B) of the Low-Income Home Energy Assistance Act of 1981.

1. Agency completes the "To" section of the form entering the non-regulated utility company information.
2. Agency completes the "From" section of the form entering the agency's name, address, and contact person.
3. Agency enters the list of client information, including utility account # and amount of payment.
4. Agency enters "Total Payments" amount and the "Check Number" information which corresponds to data from Step 3.
5. Agency forwards form to identified non-regulated utility company for review and completion.
6. Upon return of form from utility company, Agency reviews and verifies the amount credited for each client.
7. Agency retains this form on file for monitoring purposes.

Contractor's equivalent form or process is allowed, but must be pre-approved by CSD.

State of California
DEPARTMENT OF COMMUNITY SERVICES AND DEVELOPMENT
CSD 416 (Rev. 04/18/18)

ECIP/HEAP HOME ENERGY SUPPLIER ASSURANCE (NON-REGULATED UTILITY COMPANIES ONLY)

The undersigned home energy supplier hereby agrees and assures to

Agency's Name

that it will comply with the following provisions as federally-mandated under the Low-Income Home Energy Assistance Program in regard to energy fuels and related services provided to eligible households:

1. No household receiving assistance under this program will be treated adversely because of such assistance under applicable provisions of State law or public regulatory requirements;

2. Not to discriminate, either in the cost of the goods supplied or in the services provided, against the eligible household on whose behalf payments are made; and

3. To allow representatives of the agency referenced above, and/or the State, access to records relating to payments to households for the purpose of verification of compliance with these assurances.

Utility Company	
Name and Title (Please Print)	Telephone Number
Authorized Signature	Date

ANNUAL ECIP/HEAP HOME ENERGY SUPPLIER ASSURANCE
(NON-REGULATED UTILITY COMPANIES ONLY)
CSD 416 (Rev. 6/1/06)
Instructions

Use this form to comply with Section 2605(b)(7), items (C) and (D) of the Low-Income Home Energy Assistance Act of 1981.

1. Enter the agency name on the line provided.

2. This form must be provided to the non-regulated utility company for signature.

3. Once the form is returned from the non-regulated utility company, ensure that the form is signed and dated.

4. Retain this form for up to one year from the date of signature.

5. This form must be submitted to the non-regulated utility company for signature on an annual basis.

6. Please refer to http://www.acf.hhs.gov/programs/liheap/guidance/statute/statute.html#Sec2605 for the regulation.

OFFICE OF THE GOVERNOR

May 22, 2019

Mr. Clarence H. Carter
Director
Office of Community Services
Administration for Children and Families
U.S. Department of Health and Human Services
330 C Street, S.W.
Washington, D.C. 20201

Dear Mr. Carter:

Pursuant to 42 U.S.C. 9908(a)(1) and Title 45, Part 96.10(b) of the Code of Federal Regulations, I hereby delegate signature authority to Linné K. Stout, Director of the State of California's Department of Community Services and Development, and her successor, for the purposes of submitting the application and certifying compliance with federal assurances relating to the Community Services Block Grant and Low-Income Home Energy Assistance Program.

Sincerely,

Gavin Newsom
Governor of California

2021 LIHEAP County Base Benefit Amounts (BBA)
Benefit Amounts Listed Apply to Household Size 1 ONLY

Agency Name	Service Area	Poverty Group I Benefit	Poverty Group II Benefit	Poverty Group III Benefit	Poverty Group IV Benefit
Spectrum Community Services	ALAMEDA	$289	$228	$192	$156
El Dorado County, Health and Human Services	ALPINE	$418	$331	$279	$226
	EL DORADO	$494	$391	$329	$267
Amador-Tuolumne CAA	AMADOR	$418	$331	$279	$226
	CALAVERAS	$401	$318	$267	$217
	TUOLUMNE	$399	$316	$266	$216
Butte County CAA	BUTTE	$391	$310	$261	$212
Glenn County Human Resource	COLUSA	$390	$308	$260	$211
	GLENN	$397	$314	$265	$215
	TRINITY	$462	$365	$308	$250
Contra Costa	CONTRA COSTA	$357	$283	$238	$193
Del Norte Senior Center	DEL NORTE	$474	$375	$316	$257
Fresno County EOC	FRESNO	$392	$310	$261	$212
Redwood CAA	HUMBOLDT	$370	$293	$246	$200
Campesinos Unidos, Inc.	IMPERIAL	$336	$266	$224	$182
	SAN DIEGO	$284	$225	$189	$154
IMACA	INYO	$389	$308	$260	$211
	MONO	$379	$300	$253	$205
CAP of Kern County	KERN	$357	$283	$238	$193
Kings CAO, Inc.	KINGS	$352	$279	$235	$191
North Coast Energy Services	LAKE	$458	$363	$306	$248
	MENDOCINO	$391	$310	$261	$212
	NAPA	$354	$280	$236	$192
	SOLANO	$369	$292	$246	$200
	SONOMA	$325	$257	$216	$176
	YOLO	$306	$243	$204	$166
Lassen Economic Development Corp.	LASSEN	$438	$347	$292	$237
Maravilla Foundation	LOS ANGELES	$359	$284	$239	$194
PACE	LOS ANGELES	$359	$284	$239	$194
Long Beach CSDC	LOS ANGELES	$359	$284	$239	$194
CAP of Madera County	MADERA	$391	$310	$261	$212
Community Action Marin	MARIN	$396	$313	$264	$214

Mariposa County Human Services Dept	MARIPOSA	$390	$308	$260	$211
Merced County CAA	MERCED	$375	$297	$250	$203
T.E.A.C.H.	MODOC	$396	$314	$264	$215
Central Coast Energy Services	MONTEREY	$267	$211	$178	$144
	SAN FRANCISCO	$269	$213	$179	$146
	SAN MATEO	$328	$260	$219	$178
	SANTA CRUZ	$313	$248	$209	$170
Project GO, Inc.	NEVADA	$527	$417	$352	$286
	PLACER	$428	$339	$286	$232
CAP of Orange County	ORANGE	$318	$252	$212	$172
Plumas County. CDC	PLUMAS	$345	$273	$230	$187
	SIERRA	$365	$289	$243	$198
CAP of Riverside County	RIVERSIDE	$355	$281	$237	$192
Community Resource Project	SACRAMENTO	$375	$297	$250	$203
	SUTTER	$403	$319	$269	$218
	YUBA	$398	$315	$265	$216
San Benito County Dept. of CSWD	SAN BENITO	$310	$246	$207	$168
CAP of San Bernardino County	SAN BERNARDINO	$321	$254	$214	$174
MAAC	SAN DIEGO	$284	$225	$189	$154
San Joaquin County Dept. of ACS	SAN JOAQUIN	$408	$323	$272	$221
CAP of San Luis Obispo County	SAN LUIS OBISPO	$321	$254	$214	$174
CAC of Santa Barbara County	SANTA BARBARA	$301	$238	$201	$163
Sacred Heart Community Service	SANTA CLARA	$313	$248	$209	$169
SHHIP	SHASTA	$466	$369	$311	$252
	TEHAMA	$430	$340	$287	$233
Great Northern Corporation	SISKIYOU	$458	$362	$305	$248
CVOC	STANISLAUS	$437	$346	$291	$236
C-SET	TULARE	$333	$264	$222	$180
Community Action of Ventura County	VENTURA	$290	$229	$193	$157

2021

HEAP and FAST TRACK Base Benefit Amounts (BBA)

SAMPLE COUNTY

Household's Monthly Income Guidelines and Poverty Group

HH Size	Poverty Group 1	Poverty Group 2	Poverty Group 3	Poverty Group 4
1	$ 200	$ 180	$ 150	$ 130
2	$ 219	$ 199	$ 169	$ 149
3	$ 238	$ 218	$ 188	$ 168
4	$ 257	$ 237	$ 207	$ 187
5	$ 276	$ 256	$ 226	$ 206
6	$ 295	$ 275	$ 245	$ 225
7	$ 295	$ 275	$ 245	$ 225
8	$ 295	$ 275	$ 245	$ 225
9	$ 295	$ 275	$ 245	$ 225
10	$ 295	$ 275	$ 245	
11	$ 295	$ 275	$ 245	
12	$ 295	$ 275	$ 245	
13	$ 295	$ 275		
14	$ 295	$ 275		
15	$ 295	$ 275		
16	$ 295	$ 275		
17	$ 295	$ 275		
18	$ 295			
19	$ 295			
20	$ 295			
21	$ 295			
22	$ 295			
23	$ 295			
24	$ 295			
25	$ 295			

1 - The payment amounts for each county from Benefit Matrix 1 are applied to household size 1 on the payment table

2. Household sizes 2 through 6 each receive an additional $19.

3. Household sizes 6 and higher received the same payment amounts

Sample Scenario: If County ABC's payment amounts from Benefit Matrix 1 are $200, $180, $150 and $130, this payment table shows those payment amounts being applied to household size 1. Additionally, the payment amounts for household sizes 2 and higher are illustrated. This follows Program Year 2021's utility assistance payment determinations. Household sizes 2 through 6 each receiving an additional $19. Household sizes 6 and higher receive the same payment amount.

2021 Low-Income Home Energy Assistance Program (LIHEAP) State Plan Proposed Changes

Section	Question	2020 State Plan	2021 State Plan Proposed Changes
Section 1	**Program Components -**		
1.1	**Check which components you will operate under the LIHEAP program. (Note: You must provide information for each component designated here as requested elsewhere in this plan.)**	Heating: Start Date: 10/01/19 End Date: 9/30/20 Cooling: Start Date: 10/01/19 End Date: 9/30/20 (Cooling added) Crisis: Start Date: 10/01/19 End Date: 9/30/20 Weatherization: Start Date: 10/01/19 End Date: 9/30/20	Start Date: 10/01/20 End Date: 9/30/21 Start Date: 10/01/20 End Date: 9/30/21 Start Date: 10/01/20 End Date: 9/30/21 Start Date: 10/01/20 End Date: 9/30/21
	Provide further explanation for the dates of operation, if necessary	The 2020 Contract Term runs from 10/01/2019 through 06/30/2021. The intent of the contract term is to ensure continuation of services in the event that federal funds are not released by 10/1/2019. Local Service Providers are expected to expend funds by November 2020.	The 2021 Contract Term runs from 10/01/2020 through 06/30/2022. The intent of the contract term is to ensure continuation of services in the event that federal funds are not released by 10/1/2020. Local Service Providers are expected to expend funds by November 2021.
1.2	**Estimate what amount of available LIHEAP funds will be used for each component that you will operate: The total of all percentages must add up to 100%**	Heating assistance 20% Cooling assistance 6% Crisis assistance 34.00% Weatherization assistance 15.00% Carryover to the following federal fiscal year 10.00% Administrative and planning costs 10.00% Services to reduce home energy needs including needs assessment (Assurance 16) 5.00% Used to develop and implement leveraging activities 0% TOTAL 100% Note: Heating figures have been split with Cooling as an estimate. Original figure 26%)	Heating assistance 21% Cooling assistance 6% Crisis assistance 33% Weatherization assistance 15% Carryover to the following federal fiscal year 10% Administrative and planning costs 10% Services to reduce home energy needs including needs assessment (Assurance 16) 5% Used to develop and implement leveraging activities 0% TOTAL 100%
Section 2	**Heating Assistance -**		
2.6	**Describe estimated benefit levels for FY2021**	2020: Minimum $152 Maximum $1000	2021: Minimum $144 Maximum $1000

Section 3	**Cooling Assistance**		
3.6	**Describe estimated benefit levels for FY2020**	Minimum $152 Maximum $1000	Minimum $144 Maximum $1000
Section 4	**Crisis Assistance**		
4.8	**How do you handle crisis situations?** **Other - Describe:**	The Crisis Program is limited to four activities: 1. Fast Track (electric and gas) utility payments 2. Energy Crisis Intervention Program Wood, propane and oil (ECIP WPO) payments 3. Heating and cooling services (HCS) 4. Severe Weather Energy Assistance and Transportation Services (SWEATS) Fast Track benefits are determined by the Local Service Providers, but payments to the utility companies are processed, centrally, by CSD, where ECIP WPO assistance, HCS and SWEATS benefits are provided locally. Local Service Providers have the ability to increase the Fast Track base amount by adding a supplemental benefit. The total benefit amount cannot exceed the total amount of the entire utility bills (to include energy charges, reconnection fees, and other assessed utility fees/surcharges to alleviate the crisis situation) or $1,000, whichever is less. ECIP WPO benefits are determined at the local level based on clients inability to pay for essential firewood, oil or propane. The amount of the benefit is based on the cost to resolve the crisis. HCS services provide payment for energy-related repairs or replacement of non-functioning heating, cooling appliances and water-heating appliances. The benefit amount is based on the cost of the repair or replacement, up to the maximum amount as determined annually. SWEATS services provide payment to address energy-related emergency needs of low-income households affected by a natural disaster. Typical services include additional utility assistance, temporary housing services, transportation services and temporary heating/cooling devices. The amount of the benefit may vary depending on the benefit offered.	The Crisis Program is limited to five activities: 1. Fast Track (electric and gas) utility payments 2. Energy Crisis Intervention Program Wood, propane and oil (ECIP WPO) payments 3. Heating and cooling services (HCS) 4. Severe Weather Energy Assistance and Transportation Services (SWEATS) 5. Public Safety Power Shutoff (PSPS) Pilot Program SWEATS services provide payment to address energy-related emergency needs of low-income households affected by a natural disaster and PSPS. Typical services include additional utility assistance, temporary housing services, transportation services, temporary heating/cooling devices, and battery backup devices. The amount of the benefit may vary depending on the benefit offered. PSPS Emergency Preparedness Pilot services low-income households medically vulnerable to the effects of energy-related emergencies and residing in designated High Fire Risk Areas. As a pilot, it is designed to collect detailed reporting in order to further develop the PSPS Emergency Preparedness component and to aid LSPs in leveraging other resources to implement Emergency Preparedness services. Services include household emergency risk assessment, PSPS preparedness education, emergency preparedness supplies, and backup power appliances.
4.13	**Do you provide in-kind and/or other forms of benefits? If yes, please describe.**	Space heaters are allowable under the Emergency Heating and Cooling Program and the Severe Weather Energy Assistance and Transportation Program.	Space heaters are allowable under the Emergency Heating and Cooling Program. Evaporative coolers, heaters, fans, battery power backup devices, and generators are allowable under the Severe Weather Energy Assistance and Transportation Program.
Section 5	**Weatherization**		
5.8	**Other: Explanation**	CSD will implement the new Priority Plan for 2020 that prioritizes applicants based on income, energy burden, and vulnerable population (elderly, disabled, and families with young children).	CSD will implement the new Priority Plan for 2021 that prioritizes applicants based on income, energy burden, and vulnerable population (elderly, disabled, and families with young children).
5.10	**What is the maximum LIHEAP Weatherization benefit/expenditure per household?**	**Add Attachment:** The current max average per unit under LIHEAP is $7212.	**Add Attachment:** The current max average per unit under LIHEAP is $7669.
5.11	**Section 5.11 - What LIHEAP weatherization measures do you provide ? (Check all categories that apply.) Other: Describe**	**Added:** Shutters Window Repair and Replacement **Removed:** Solar Water Heater Installation	**Added:** Infiltration Reduction (previous Infiltration Reduction Measures including Caulking; Cover Plate Gaskets; Glass Replacement; Minor Envelope Repair; Weatherstripping; and Vent Covers, Interior have been combined into a single Infiltration Reduction Measure) LED Downlight Retrofit Kits; LED-Hard-Wired Lights – Exterior – Porch Light; LED-Hard Wired Lights – Exterior - Security Light; LED Hard-Wired Lights – Interior – Ceiling; LED Hard Wired Lights – Interior Vanity; and LED Hard-Wired Lights – Interior – Wall/Sconce Whole House Fans **Removed:** Compact Fluorescent Lamps Fluorescent Torchiere Lamp Replacement

Section 10	**Program, Fiscal Monitoring, and Audit - Assurance 10**		
10.3	**Describe any audit finding rising to the level of material weakness or reportable condition cited in the A-133 audits. Grantee monitoring assessments, inspector general reviews, or other government agency reviews of the LIHEAP agency from the most recently audited fiscal year**	No findings for 2019.	No findings for 2020.
10.6	**Explain, or attach a copy of your local agency monitoring schedule and protocol.**	Updated monitoring scope (attached)	Updated monitoring scope (attached)
10.12	**How many local agencies are currently on corrective action plans for financial accounting or administrative issues?**	6	0
Section 11	**Timely and Meaningful Public Participation - Assurance 12**		
11.3	**List the date and location(s) that you held public hearing(s) on the proposed use and distribution of your LIHEAP funds?**	This is left blank in the Draft Plan. This information gets filled in on the Final Plan	This is left blank in the Draft Plan. This information gets filled in on the Final Plan
11.4	**How many parties commented on your plan at the hearing(s)?**	This is left blank in the Draft Plan. This information gets filled in on the Final Plan	This is left blank in the Draft Plan. This information gets filled in on the Final Plan
11.5	**Summarize the comments you received at the hearing(s).**	This is left blank in the Draft Plan. This information gets filled in on the Final Plan	This is left blank in the Draft Plan. This information gets filled in on the Final Plan
11.6	**What changes did you make to your LIHEAP plan as a result of the comments received at the public hearing(s)?**	This is left blank in the Draft Plan. This information gets filled in on the Final Plan	This is left blank in the Draft Plan. This information gets filled in on the Final Plan
Section 13	**Reduction of home energy needs - Assurance 16**		
13.6	**How many households received these services?**	210,626	215,942
	Plan Attachments		
	Delegation Letter	Included	Included
	Heating benefit Matrix	Included	Included
	Cooling Benefit Matrix	Included	Included
	Minutes, notes or transcripts of public hearing(s).	To be included with the Final State plan after public hearing	To be included with the Final State plan after public hearing