

ATTACHMENT 5

SAMPLE PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT TEMPLATE
 Low Income Home Energy Assistance Program (LIHEAP)

ABSTRACT:

HHS is requiring further detail from Grantees on their FY2012 plans for preventing and detecting fraud, abuse, and improper payments. HHS is also requiring that Grantees highlight and describe all elements of this FY2012 plan which represent improvements or changes to the Grantees' FY2011 plan for preventing and detecting fraud, abuse and improper payment prevention.

Instructions: Please provide full descriptions of the Grantee's plans and strategy for each area, and attach/reference excerpts from relevant policy documents for each question/column. Responses must explicitly explain whether any changes are planned for the new FY.

State, Tribe or Territory (and grant official): California		Date/Fiscal Year: 9/1/11 2011/2012	
RECENT AUDIT FINDINGS			
Describe any audit findings of material weaknesses and reportable conditions, questioned costs and other findings cited in FY2011 or the prior three years, in annual audits, Grantee monitoring assessments, Inspector General reviews, or other Government Agency reviews of LIHEAP agency finances.	Please describe whether the cited audit findings or relevant operations have been resolved or corrected. If not, please describe the plan and timeline for doing so in FY2012.	If there is no plan in place, please explain why not.	Necessary outcomes from these systems and strategies
<i>Please refer to Attachment 1 for audit results</i>	All recommendations have been addressed	NA	<i>The timely and thorough resolution of weaknesses or reportable conditions as revealed by the audit.</i>

According to the Paperwork Reduction Act Of 1995 (Pub. L. 104-13), public reporting burden for this collection of information is estimated to average 1 hours 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.

ATTACHMENT 5

COMPLIANCE MONITORING			
Describe the Grantee's FY 2011 strategies that will continue in FY 2012 for monitoring compliance with State and Federal LIHEAP policies and procedures by the Grantee and local administering agencies.	Please highlight any strategies for compliance monitoring from your plan which will be newly implemented as of FY 2012.	If you don't have a firm compliance monitoring system in place for FY 2011, please describe how the State is verifying that LIHEAP policy and procedures are being followed.	Necessary outcomes from these systems and strategies
<p><i>CSD conducts on-site compliance monitoring of LIHEAP agencies every other year, and performs quarterly desk reviews. The general scope for 2011 CSD Energy Programs on-site monitoring includes, but is not limited to, the following areas:</i></p> <p>Administrative Review</p> <ul style="list-style-type: none"> <i>o Board membership and board meeting minutes evaluation</i> <i>o Review of separation of duties</i> <i>o Review and verify adherence to conflict of interest, procurement, inventory, and record retention policies</i> <p>Subcontractor Oversight Review</p> <ul style="list-style-type: none"> <i>o Review subcontractor agreement to ensure compliance with LIHEAP contract requirements</i> <i>o Verify that contractor has adequate subcontractor oversight</i> <p>Fiscal and Performance Review</p> <ul style="list-style-type: none"> <i>o Validate claims for reimbursements</i> <i>o Obtain and evaluate cost allocation plan</i> <i>o Verify and evaluate billing process</i> <p>Programmatic Review</p> <ul style="list-style-type: none"> <i>o Verify resolution of prior monitoring findings and implementation of recommendations</i> <i>o Conduct client file review to verify client and dwelling eligibility</i> <i>o Address issue or concerns identified during the course of the year such as client complaints or audit concerns</i> <i>o Review training logs for updates and verification of completion</i> <p>Quarterly Desk Review</p> <p><i>Field monitors conduct quarterly desk reviews to actively monitor agency expenditure performance, resolution of corrective actions, reporting requirements and data discrepancies.</i></p>	<p>No changes anticipated for FY2012</p>	<p>NA</p>	<p><i>A sound methodology, with a schedule for regular monitoring and a more effective monitoring tool to gather information.</i></p>

ATTACHMENT 5

FRAUD REPORTING MECHANISMS			
For FY 2011 activities continuing in FY 2012, please describe all (a) mechanisms available to the public for reporting cases of suspected LIHEAP fraud, waste or abuse [These may include telephone hotlines, websites, email addresses, etc.]; (b) strategies for advertising these resources.	Please highlight any tools or mechanisms from your plan which will be newly implemented in FY 2012, and the timeline for that implementation.	If you don't have any tools or mechanisms available to the public to prevent fraud or improper payments, please describe your plan for involving all citizens and stakeholders involved with your program in detecting fraud.	Necessary outcomes of these strategies and systems
<i>The Department operates a toll free line available to the public to receive information regarding possible fraud.</i>	No change anticipated for FY2012	NA	<i>Clear lines of communication for citizens, grantees, clients, and employees to use in pointing out potential cases of fraud or improper payments to State administrators.</i>
Please refer to CSD's website www.csd.ca.gov			
VERIFYING APPLICANT IDENTITIES			
Describe all FY 2011 Grantee policies continuing in FY2012 for how identities of applicants and household members are verified.	Please highlight any policy or strategy from your plan which will be newly implemented in FY 2012.	If you don't have a system in place for verifying applicant's identities, please explain why and how the Grantee is ensuring that only authentic and eligible applicants are receiving benefits.	Necessary outcomes from these systems and strategies
<i>CSD uses the SSN as an identifier, therefore, the SSN is requested from all applicants. However, it is not a requirement to receive services. An applicant may refuse to submit their SSN. If no SSN is submitted then a picture ID is required to verify identity. Names, SSN and date of birth are not required for all household members only for the applicant. The SSN is not verified other than the Death Match File.</i>	No new policy anticipated for FY 2012	NA	<i>Income and energy supplier data that allow program benefits to be provided to eligible individuals.</i>
Please refer to CSD's website www.csd.ca.gov ; link to the LIHEAP Verification and Eligibility Guide, Citizenship and Alien Status for Public Agencies, pages 9-11 and 20-21			

ATTACHMENT 5

SOCIAL SECURITY NUMBER REQUESTS			
Describe the Grantee's FY 2012 policy in regards to requiring Social Security Numbers from applicants and/or household members applying for LIHEAP benefits.	Please describe whether the State's policy for requiring or not requiring Social Security numbers is new as of FY2012, or remaining the same.	If the Grantee is not requiring Social Security Numbers of LIHEAP applicants and/or household members, please explain what supplementary measures are being employed to prevent fraud.	Necessary outcomes from these systems and strategies
<i>Intake and data entry occurs at the local level. SSNs are optional but are still requested from all applicants. It is not required of other household members. If the applicant refuses to submit their SSN, the applicant's identity must be established through a picture ID and then the intake form and all supporting documents are faxed to CSD to be researched, a 9 digit number is assigned and faxed back to the agency, who will enter the application using the 9 digit number in place of a SSN.</i>	No changes anticipated for FY2012	NA	<i>All valid household members are reported for correct benefit determination.</i>
Please refer to CSD's website www.csd.ca.gov ; link to the Verification and Eligibility Guide, Processing Applications without a Social Security Number, page 20 and 21.			
CROSS-CHECKING SOCIAL SECURITY NUMBERS AGAINST GOVERNMENT SYSTEMS/DATABASES			
Describe if and how the Grantee used existing government systems and databases to verify applicant or household member identities in FY 2011 and continuing in FY 2012. (Social Security Administration Enumeration Verification System, prisoner databases, Government death records, etc.)	Please highlight which, if any, policies or strategies for using existing government databases will be newly implemented in FY 2012.	If the Grantee won't be cross checking Social Security Numbers and ID information with existing government databases, please describe how the Grantee will supplement this fraud prevention strategy.	Necessary outcomes from these systems and strategies
<i>CSD's database uses the Death Match file from SSA to verify all SSNs/last names for the applicant only. The audit is performed twice, once at data entry and again just prior to approval for payment. If a match occurs, the database will not accept entry of that SSN. Agencies must research and follow up to make necessary corrections. If an error has occurred on the SSA file, CSD can temporarily override and accept the SSN. It is then imperative that the client contact SSA and correct the error.</i>	No new policy anticipated for FY 2012	NA	<i>Use of all available database systems to make sound eligibility determination.</i>

ATTACHMENT 5

VERIFYING APPLICANT INCOME			
Describe how the Grantee or designee used State Directories of new hires or similar systems to confirm income eligibility in FY 2011 and continuing in FY 2012.	Please highlight any policies or strategies for using new hire directories which will be newly implemented in FY 2012.	If the Grantee won't be using new hire directories to verify applicant and household member incomes how will the Grantee be verifying the that information?	Necessary outcomes from these systems and strategies
<i>Currently CSD does not use the State Directories for new hires to confirm income eligibility. Eligibility is based on the stated income amount and supporting documentation submitted by the applicant. New for 2011 any member of the household 18 years or older is required to sign a self certification form if they report no income. Earned income from a minor under 18 is excluded. Other exclusions apply as required by federal law.</i>	No changes anticipated for FY2012	NA	<i>Effective income determination achieved through coordination across program lines.</i>
Please refer to CSD's website www.csd.ca.gov ; link to the Verification and Eligibility Guide, Client File Documentation and Income Verification, pages 22-45			
PRIVACY-PROTECTION AND CONFIDENTIALITY			
Describe the financial and operating controls in place in FY 2011 that will continue in FY 2012 to protect client information against improper use or disclosure.	Please highlight any controls or strategies from your plan which will be newly implemented as of FY 2012.	If you don't have relevant physical or operational controls in place to ensure the security and confidentiality of private information disclosed by applicants, please explain why.	Necessary outcomes from these systems and strategies
<i>Sub-grantees are contractually bound to maintain the confidentiality of all LIHEAP applicant and household information. CSD Field Representatives monitors verify confidentiality procedures during field visits. All CSD employees must sign and follow the Computer Security Policy.</i>	No new policy anticipated for FY 2012	NA	<i>Clear and secure methods that maintain confidentiality and safeguard the private information of applicants.</i>
Please refer to CSD's website www.csd.ca.gov ; link to the Verification and Eligibility Guide, Confidentiality of Social Security Numbers and Client File Documentation page 22, also refer to Attachment 2 , 3 and 6			

ATTACHMENT 5

LIHEAP BENEFITS POLICY			
Describe FY 2011 Grantee policies continuing in FY 2012 for protecting against fraud when making payments, or providing benefits to energy vendors on behalf of clients.	Please highlight any fraud prevention efforts relating to making payments or providing benefits which will be newly implemented in FY 2012.	If the Grantee doesn't have policy in place to protect against improper payments when making payments or providing benefits on behalf of clients, what supplementary steps is the Grantee taking to ensure program integrity.	Necessary outcomes from these systems and strategies
<i>CSD's database has validations for preventing duplicate service address, name, SSN, phone number and utility account number for the utility receiving the benefit. 97% of all benefits are directly sent to utility companies to be applied to customer accounts. Utility companies return benefits to CSD that could not be credited to the appropriate accounts. The remaining 3% of benefits are issued to individuals with utilities included in rent and customers of non-direct payment utilities in the form of a paper warrant, which is audited by the State Controller's Office.</i>	No new policy anticipated for FY 2012	NA	<i>Authorized energy vendors are receiving payments on behalf of LIHEAP eligible clients.</i>
PROCEDURES FOR UNREGULATED ENERGY VENDORS			
Describe the Grantee's FY 2011 procedures continuing in FY 2012 for averting fraud and improper payments when dealing with bulk fuel dealers of heating oil, propane, wood and other un-regulated energy utilities.	Please highlight any strategies policy in this area which will be newly implemented in FY 2012.	If you don't have a firm plan for averting fraud when dealing with unregulated energy vendors, please describe how the Grantee is ensuring program integrity.	Necessary outcomes from these systems and strategies
<i>CSD 416 Annual ECIP/HEAP Home Energy Supplier Assurance, completed by all non regulated vendors, assures that all non-regulated companies will follow the provisions as federally-mandated under the LIHEAP program in regard to energy fuels and related services provided to eligible households. CSD 415 Payment Request and Confirmation - completed by the vendor, confirms that the clients' account has been credited. Sub grantees are required to notify applicant of the benefit amount they will be receiving. CSD Field Representatives monitor to verify that the forms are completed and retained in the client file.</i>	No changes anticipated for FY2012	NA	<i>Participating vendors are thoroughly researched and inspected before benefits are issued.</i>
See Attachment 4 and 5			

ATTACHMENT 5

VERIFYING THE AUTHENTICITY OF ENERGY VENDORS			
Describe Grantee FY 2011 policies continuing in FY 2012 for verifying the authenticity of energy vendors being paid under LIHEAP, as part of the Grantee's procedure for averting fraud.	Please highlight any policies for verifying vendor authenticity which will be newly implemented in FY 2012.	If you don't have a system in place for verifying vendor authenticity, please describe how the Grantee can ensure that funds are being distributed through valid intermediaries?	Necessary outcomes from these systems and strategies
<i>CSD documents authenticity of energy vendors by collecting the Federal Employer ID number for gas and electric vendors</i>	No changes anticipated for FY2012	NA	<i>An effective process that effectively confirms the existence of entities receiving federal funds.</i>
TRAINING AND TECHNICAL ASSISTANCE			
In regards to fraud prevention, please describe elements of your FY 2011 plan continuing in FY 2012 for training and providing technical assistance to (a) employees, (b) non-governmental staff involved in the eligibility process, (c) clients, and (d) energy vendors.	Please highlight specific elements of your training regimen and technical assistance resources from your plan which will represent newly implemented in FY 2012.	If you don't have a system in place for anti-fraud training or technical assistance for employees, clients or energy vendors, please describe your strategy for ensuring all employees understand what is expected of them and what tactics they are permitted to employ.	Necessary outcomes from these systems and strategies
<i>Mandatory fraud prevention training is provided to all CSD staff. All CSD staff must sign the Computer Security Policy accepting responsibilities regarding computer security. CSD conducts webinars and trainings on written policy and program requirements to ensure sub grantees are aware of implementation requirements to prevent instances of fraud.</i>	No changes anticipated for FY2012	NA	<i>The timely and thorough resolution of weaknesses or reportable conditions as revealed by the audit.</i>
See Attachment 6			

ATTACHMENT 5

AUDITS OF LOCAL ADMINISTERING AGENCIES			
Please describe the annual audit requirements in place for local administering agencies in FY 2011 that will continue into FY 2012.	Please describe new policies or strategies to be implemented in FY 2012.	If you don't have specific audit requirements for local administering agencies, please explain how the Grantee will ensure that LIHEAP funds are properly audited under the Single Audit Act requirements.	Necessary outcomes from these systems and strategies
<p><i>Single Audit Act</i> -Agencies are required to submit Single Audit Report(SAR) in accordance with the provisions of Office of Management and Budget (OMB) Circular A-133, "Audits of States, Local - Governments, and Non-Profit Organizations," Subpart D, Section 400(d), published June 27, 2003. - Administering agencies are required to review the SAR within six months of receipt - Program specific audits are required for agencies falling below the OMB 133 threshold</p>	<p>No changes anticipated for FY2012</p>	<p>NA</p>	<p><i>Reduce improper payments, maintain local agency integrity, and benefits awarded to eligible households.</i></p>
<p>Please refer to CSD's website www.csd.ca.gov; link to 2011 LIHEAP Contract pages A3, C1, and D5.</p>			

Attachment – page 8

Additional Information

Please attach further information that describes the Grantee's Program Integrity Policies, including supporting documentation from program manuals, including pages/sections from established LIHEAP policies and procedures.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 1

Recent Audit Findings

Prior Year Audit Finding Resolutions

4700 - Department of Community Services and Development

Finding Number	Federal Program	Category of Finding	Finding Summary	Status of Corrective Action (Please see legend below for definitions)			
				Fully Corrected (√ only)	Partially Corrected	Corrective Action Plan (Provide details)	Date Fully Corrected
2009-5-8	93.568	Eligibility	Local agencies did not always maintain sufficient documentation such as applicants' monthly income or citizenship status to substantiate their assistance eligibility determinations. Also, CSD allows flexibility when calculating monthly income amounts which could lead to local agencies inappropriately approving applicants whose monthly income would otherwise make them ineligible for assistance. Also, public local agencies did not always obtain sufficient citizenship documents for applicants.	✓		Develop tools to assist intake workers with acceptable documentation	5/12/2010
2009-7-13	93.568	Earmarking	Community Services lacks sufficient internal controls to ensure that it meets earmarking requirements. Community Services does not have a mechanism in place to track final expenditures related to earmarking requirements.		✓	CSD will phase-in an enhancement to an application system (i.e., Expenditure Activity Reporting System) that will automatically monitor, track and report on the level of earmark usage per program, contract and program year.	
2009-9-7	93.568	Procurement and Suspension and Debarment	Community Services did not comply with the suspension and debarment requirements in the Administration for Children and Families grants' terms and conditions. Community Services did not consult the federal Excluded Parties List System (EPLS) to ensure that the subrecipients were eligible for funding before it disbursed funds to them.	✓		CSD has issued a directive that contracts analyst will annually or at the start of a new contractor's term with CSD verify that the firm and any principals and board members are not included on the Excluded Parties List System by verifying via http://www.epls.gov .	6/14/2010
2009-12-19	93.568	Reporting	Community Services lacks adequate internal controls to ensure that proper federal reporting requirements are met. Community Services' policies and written procedures do not include procedures to reconcile the federal share of program outlays from spreadsheets to official accounting records.		✓	CSD has contracted with Cooperative Personnel Services (CPS) to develop Policies and Procedures for the Department. In addition, CPS will train CSD staff to maintain and update policies and procedures.	

Finding Number	Federal Program	Category of Finding	Finding Summary	Fully Corrected (√ only)	Partially Corrected	Corrective Action Plan (Provide details)	Date Fully Corrected
2009-14-3	93.568	Subrecipient Monitoring	Community Services' audit services unit (ASU) did not always ensure that it issued management decisions on audit findings within six months of receipt of subrecipients' OMB Circular A-133 reports.		✓	In May 2010, CSD entered into a contract with the Department of Finance to assist in meeting its obligation to review single audits within the required six months.	

LEGEND FOR STATUS OF CORRECTIVE ACTION
FULLY CORRECTED: If audit findings were fully corrected and the recommendation(s) were implemented, explain what steps were taken to correct the finding. If the finding is no longer valid, please describe the circumstances. If corrective action is significantly different from corrective action previously reported in the fiscal year 2008-09 Single Audit Report, then provide an explanation. If this category is not applicable, please such with N/A.
PARTIALLY CORRECTED: If audit findings are partially corrected, describe the planned corrective action as well as any partial corrective action taken. If corrective action is significantly different from corrective action previously reported in the fiscal year 2008-09 Single Audit Report, then provide an explanation. If this category is not applicable, please indicate such with N/A.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 2

Privacy-Protection and Confidentiality

MANAGEMENT MEMO

SUBJECT: SAFEGUARDING AGAINST AND RESPONDING TO A BREACH OF SECURITY INVOLVING PERSONAL INFORMATION	NUMBER: MM 08-11
	DATE ISSUED: NOVEMBER 6, 2008
	EXPIRES: UNTIL RESCINDED
REFERENCES: CALIFORNIA INFORMATION PRACTICES ACT OF 1977 (CIVIL CODE SECTIONS 1798 ET. SEQ); STATE ADMINISTRATIVE MANUAL (SAM) SECTIONS 5100 AND 5300 THROUGH 5399	ISSUING AGENCY: OFFICE OF INFORMATION SECURITY AND PRIVACY PROTECTION

BACKGROUND AND PURPOSE

Government Code section 11549.3 charges the Office of Information Security and Privacy Protection (OISPP) with responsibility for the creation, updating, and publishing of information security and privacy policies, standards, and procedures directing state agencies to effectively manage security and risk for information and information technology (as defined).

The purpose of this Management Memo (Memo) is to announce a new policy requirement and procedural directive related to a state agency’s response to a breach of security involving personal information. It also serves to reinforce state agency responsibilities under existing law and state policy for safeguarding personal information collected, used, maintained, and/or held in custodianship in conjunction with the administration of state programs and services, and to clarify existing security incident management policies and procedures.

Safeguarding against and preventing security breaches involving personal information is essential to maintaining the public’s trust in government. Failure to protect personal information can place people in jeopardy in a variety of ways, including identity theft, damage to reputation, and physical injury.

While ultimate responsibility rests with agency heads, every employee plays a role in the protection of personal information. This Memo should receive the widest possible distribution within state agencies, and each organization and individual must understand their specific responsibilities for implementing and complying with information security and privacy requirements and procedures.

GENERAL POLICY

Longstanding policies articulated in State Administrative Manual (SAM) and law, including but not limited to SAM Sections 5100 and 5300 through 5399, and the California Information Practices Act (IPA) of 1977 (Civil Code sections 1798 et seq.), require all state agencies to establish:

- Ongoing data inventory and classification procedures for all records held by the agency. (SAM section 5320.5 and Chapter 1600).
- Administrative, technical, and physical safeguards to appropriately ensure the security (confidentiality, integrity, and availability) of those records and to protect against anticipated threats or hazards that could result in any injury. (SAM sections 5310 and 5325, and Civil Code section 1798.21).
- Rules of conduct for any person involved in the design, development, operation, use, disclosure, maintenance, and destruction of records

STATE ADMINISTRATIVE MANUAL

containing personal information. (Management Memo 06-12, SAM sections 5310 and 5325, and Civil Code section 1798.20).

- Ongoing training and instruction to any persons involved in the design, development, operation, use, disclosure, maintenance, and destruction of records containing personal information about the rules and consequences of noncompliance. (SAM section 5325 and Civil Code section 1798.20).
- Encryption of portable computing devices and media that contain confidential, personal and sensitive information. (SAM section 5345.2)
- Use of the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. (SAM section 5100). 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) for Federal computer systems. These standards and guidelines are issued by 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. Guidance documents and requirements for implementing these standards include, without limitation, those related to the [validation of cryptographic modules](#) found in encryption products used for the protection of confidential, personal, or sensitive information.
- A process to ensure individuals are notified when a security breach involving their personal information has occurred. (SAM section 5350.3 and Civil Code section 1798.29).

PERSONAL INFORMATION DEFINED

The IPA broadly defines personal information in Civil Code section 1798.3 as "any information that is maintained by the 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."

For purposes of both the legal and state policy breach notification requirements, the subset of personal information as defined in Civil Code section 1798.29, subsections (e) through (f) is used and hereinafter referred to as "notice-triggering" information.

EXISTING SAFEGUARD REQUIREMENTS

The following are particularly important requirements within the existing legal and policy framework that state agencies should already have implemented to safeguard personal information:

1. Rules and Controls Limiting Access. Agencies must ensure that their access control policies and practices support the principle of "least privilege" and appropriate segregation of duties. Least privilege refers to the granting of employee access to personal information or systems based

on a legitimate business need to access the information in the performance of their job duties (refer to [Chapter 16, of NIST SP-800-12, An Introduction to Computer Security](#)). Agencies must also implement controls to detect and deter misuse, unauthorized access, or access that exceeds the limits of an employee's authorized access. For example, an employee may, by virtue of his or her job-related duties, have access to all records in a particular database or system, including records that may be held by the agency about those personally known to him or her (e.g., friends, family members, neighbors, etc.). However, that employee should not access those records unless specifically assigned a job-related duty in support of the processing or handling of such records. Agencies must also employ, to the extent practical, technical controls to automate compliance with these requirements. (SAM sections 5100, 5335.1, 5335.2, 5340, and 20050).

2. Employee Training. **Before** permitting access to agency information and information systems, agencies must train all employees (including managers and contracted staff) about their privacy and security responsibilities. Supervisors must also be trained about their role and responsibilities for providing day-to-day instruction, training and supervision of staff regarding their obligation to safeguard personal information. Thereafter, agencies must train employees at least once annually to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or changes in duties. Both initial and refresher training must cover acceptable rules of behavior and the consequences when rules are not followed. For agencies implementing telecommuting or telework, and other authorized remote access programs, training must include the rules of such programs. (SAM section 5325 and Civil Code section 1798.20).
3. Signed Acknowledgements. Agencies must ensure that all individuals with authorized access to personal information sign an acknowledgement at least once each year to demonstrate both their receipt of the rules and requisite training, as well as their understanding of the consequences for failure to follow the rules. (SAM section 5325).
4. Written Agreements with Third Parties. Agencies must ensure that when personal information is shared with third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties. The written agreement is to identify the applicable Federal and state laws, as well as all departmental policies, standards, procedures, and security controls that must be implemented and followed by the third party to adequately protect the information. The agreement must also require the third party, and any of its sub-contractors with whom they are authorized to share the data, to share only the minimum personal information necessary, to securely return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the state agency, and to individuals when appropriate, whenever there is a breach of personal information. (SAM sections 5310 and 5320.3, and Civil Code section 1798.19).
5. Encryption. Agencies must encrypt all confidential, personal, or sensitive data on mobile devices or media whenever that type of information is

authorized for use on such devices or media, using only NIST certified cryptographic modules (FIPS 140-2 validated products). (SAM sections 5100 and 5345.2).

6. Review and Reduce Current Personal Information Holdings. Agencies must review current holdings of all records containing personal information and ensure to the maximum extent practical, such holdings are reduced to the minimum necessary for the proper performance of a documented agency function. (Civil Code section 1798.14).
7. Review Current Forms and Other Methods of Personal Information Collection. Agencies must review all current forms, paper, and any other methods (e.g., online or telephony) used to collect personal information, to ensure the specific authority or authorization to collect such information exists, and appropriate notice is included on or with any such forms. (Civil Code section 1798.17).
8. Eliminate Unnecessary Collection and Use. When in the course of such reviews, the collection of personal information is no longer necessary for an authorized business purpose, agencies shall ensure that its collection is discontinued, and that the forms or any other methods used to collect this information are properly retired, revised, or replaced. (Civil Code section 1798.14).
9. Explore Alternatives to the Use of Social Security Numbers. Many recently enacted privacy laws prohibit the use of Social Security numbers as personal identifiers in state systems, or specifically require truncation when they must be used. All state agencies should participate in government-wide efforts to explore alternatives to the use of Social Security numbers as a personal identifier for both recipients of state programs and services, and state employees. (Civil Code sections 1798.14 and 1798.85).
10. Review Internal Controls to Safeguard Personal Information. Agencies must ensure that their risk management practices and ongoing assessments and reviews include evaluations of the adequacy of controls implemented to safeguard personal information held by the agency, and its contractors, and its other custodians with whom data may be shared. Internal controls include "Information Technology" controls, as well as administrative controls. (SAM sections 5305 to 5305.2). Further, in accordance with the California Financial Integrity and State Manager's Accountability Act (FISMA) of 1983 (Government Code Sections 13400 through 13407), "internal accounting and administrative controls are the methods through which reasonable assurances can be given that measures adopted by state agency heads to safeguard assets, check accuracy and reliability of accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies are being followed." To ensure the state FISMA requirements are fully complied with, the head of each state agency must conduct an internal review and report on the adequacy of its internal controls by December 31, of each odd numbered year to the Legislature, the State Auditor, the Governor, the Director of the Department of Finance, and the State Library. (SAM section 20060). An agency's review of personal information holdings, personal information collection methods, and internal controls to

safeguard personal information may be completed in conjunction with the agency's biennial FISMA review.

EXISTING INCIDENT MANAGEMENT AND BREACH RESPONSE REQUIREMENTS

Existing state law and state policy require agencies to carry out the following incident management and breach response responsibilities:

1. Promptly investigate incidents involving the improper dissemination of information, or the loss, damage, or misuse of information assets. Incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff and their response to, reporting on, and recovery from a variety of incidents. Incident management also includes the application of lessons learned, and the determination of, and implementation of appropriate corrective actions to prevent or mitigate the risk of similar occurrences. (SAM sections 5350 and 8643).
2. Immediately report any security incident, including any breach of personal information as defined by Civil Code Section 1798.3 (includes non notice-triggering personal information) to the California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) at (916) 657-8287. (SAM sections 5350.2 and 8643, and Government Code section 14613.7).
3. Notify individuals when a breach of their personal information was, or is reasonably believed to have been acquired by an unauthorized person. Civil Code section 1798.29, sub-sections (e) through (f) specifically require notification to individuals in breaches of unencrypted computerized personal information of a specified type (which is referred to as "notice-triggering" information). Notice-triggering information includes the first name or first initial and last name in combination with any one or more of the following data elements:
 - a. Social Security number.
 - b. Driver's license number or California Identification Card number.
 - c. Account number, 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).
 - e. Health insurance information (as defined).

While Civil Code section 1798.29 focuses on computerized data elements, the current state policy requires notification when a breach of an individual's personal information involves these same "notice-triggering" data elements or otherwise exposes individuals to substantial risk of harm, regardless of the data medium. (SAM section 5350.3).

4. Prepare and submit a written follow-up Agency Security Incident Report (SIMM 65C form) to OISPP, within ten (10) business days from the date of initial reporting to ENTAC, that describes what occurred, what steps or actions were taken to mitigate the risk of recurrence, and the cost associated with both the incident and any corrective action. (SAM sections 5350.3 and 5360.1).

STATE ADMINISTRATIVE MANUAL

NEW BREACH RESPONSE REQUIREMENTS AND PROCEDURAL DIRECTIVE

Effective immediately, any breach notification issued by a state agency, or the agency's contractor or custodian, in conjunction with a breach of state owned information assets must be submitted to OISPP for review and approval prior to its dissemination or release to affected individual(s). This process will help ensure consistency and clarity of notifications, as well as the accuracy of the privacy protection procedures and instructions provided in the notification.

While the decision to notify individuals ultimately rests with agency heads; when a breach occurs, agencies must seek guidance from, and consult with, the OISPP, as well as the agency's Legal Office, Information Security Officer and Privacy Officer/Coordinator regarding the means by which individuals will be notified.

In support of this policy, and to ensure state agencies understand their responsibilities for making notification to individuals affected by a breach, OISPP has also issued a new State Information Management Manual (SIMM) document as a procedural directive, entitled *SIMM 65D-Personal Information Breach Notification: Requirements and Decision-Making Criteria for State Agencies*. This document outlines the current breach notification requirements; the requirements for developing a protocol for internal notifications; identifies decision making criteria that must be included in a decision making procedure; and, provides a comprehensive checklist and notification templates to assist state agencies with response to a breach of personal information.

ROLES AND RESPONSIBILITIES

All state agencies and their employees, including contractors, state data custodians, and volunteer service workers, are required to adhere to these policies. Furthermore, state agencies are required to acknowledge the extent to which they are meeting these requirements in their Agency Risk Management and Privacy Program Certification, submitted annually to the OISPP. (SAM sections 5300.3, 5315.1, 5320 through 5320.4, and 5360.1).

"Agencies" includes all state agencies, departments, offices, boards, commissions, institutions, and special organizational entities unless otherwise specifically exempted by law or state policy reference. (SAM section 5300.2).

SAM AND SIMM UPDATES

Changes to the SAM will be forthcoming and will appear in the next update of the SAM. To see the substance of this policy change, you may refer to the following described documents on the OISPP Web site at: www.infosecurity.ca.gov:

1. Advance Copy of Changes to State Administrative Manual sections 5320.2, 5320.3, 5320.5, 5350, and 5350.4
2. SIMM 65D-Security Breach Involving Personal Information: Requirements and Decision Making Criteria for State Agencies

QUESTIONS

Questions regarding this Memo and related documents may be directed to OISPP at (916) 445-5239 or by email at Security@oispp.ca.gov

SIGNATURE

Original signed by Michael Saragoza, Undersecretary
For Rosario Marin, Secretary

Rosario Marin, Secretary
State and Consumer Services Agency

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 3

Privacy-Protection and Confidentiality

BUDGET LETTER

	NUMBER: 04-35
SUBJECT: SAFEGUARDING ACCESS TO STATE DATA	DATE ISSUED: November 16, 2004
REFERENCES: STATE ADMINISTRATIVE MANUAL SECTIONS 4840.4, 4841.2 4841.3	SUPERSEDES:

TO: Agency Secretaries
Department Directors
Departmental Budget Officers
Departmental Chief Information Officers
Departmental Information Security Officers
Department of Finance Budget Staff

FROM: DEPARTMENT OF FINANCE

Note: Budget Officers are requested to forward a copy of this Budget Letter (BL) to your department's Information Security Officers (ISOs) and department's Chief Information Officers (CIOs). The Finance State ISO Office will also distribute this BL separately to the ISOs and CIOs on the current contact list.

BACKGROUND

The Department of Finance (Finance) is responsible for establishing the framework for the State's information technology (IT) security policies and activities, and for IT security oversight. This BL expands upon and clarifies policy about protecting the State's information resources.

The State Administrative Manual (SAM) Section 4841.2, Information Integrity and Security, requires that each agency provide for the integrity and security of its automated files and databases. New policy in this section requires written agreements with vendors, consultants, or researchers before they are allowed access to State data.

Although some agencies already have practices in place that support these policies, it is critical that State data in all agencies be protected through good policy and practice.

POLICY

The following definition and policy are effective immediately. The changes will appear in the next update of the SAM. You may refer to Attachment I, "Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2," to see the context of this policy change.

Definition:

Non-State Entity. A business, organization, or individual that is not a State entity, but requires access to State information assets in conducting business with the State. (This definition includes, but is not limited to, researchers, vendors, consultants, and their employees, and entities associated with federal and local government and other states.)

Policy:

Each agency must provide for the integrity and security of its information assets by ensuring that responsibility for each automated file or database is defined.

Every agency must establish appropriate policies and procedures for preserving the integrity and security of each automated file or database. This requirement includes the use of agreements with non-state entities, to cover, at a minimum, the following:

- Appropriate levels of confidentiality for the data, based on data classification (see SAM section 4841.3);
- Standards for transmission and storage of the data, if applicable;
- Agreement to comply with all State policy and law regarding use of information resources and data;
- Signed confidentiality statements;
- Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which the data may be used; and
- Agreement to notify the State data owners promptly if a security incident involving the data occurs.

CONTACTS AND QUESTIONS

You may call the State ISO Office at (916) 445-5239 if you have questions about this BL or about the practices.

/s/ Veronica Chung-Ng

Veronica Chung-Ng
Program Budget Manager

Attachment

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

New text is in italics; nothing was deleted.

4840.4 DEFINITIONS

Confidential Information. Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws. See SAM Section 4841.3.

Critical Application. An application that is so important to the agency that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs.

Custodian of Information. An employee or organizational unit (such as a data center or information processing facility) acting as a caretaker or an automated file or database.

Disaster. A condition in which an information asset is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Hardening. A defense strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.

Information Assets. (1) All categories of automated information, including (but not limited to) records, files, and databases; and (2) information technology facilities, equipment (including personal computer systems), and software owned or leased by state agencies.

Information Integrity. The conditions in which information or programs are preserved for their intended purpose; including the accuracy and completeness of information systems and the data maintained within those systems.

Information Security. The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.

Owner of Information. An organizational unit having responsibility for making classification and control decisions regarding an automated file or database.

Non-State Entity. *A business, organization, or individual that is not a State entity, but requires access to State information assets in conducting business with the State. (This definition includes, but is not limited to, researchers, vendors, consultants, and their employees, and entities associated with federal and local government and other states.)*

Physical Security. The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

Privacy. The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Public Information. Any information prepared, owned, used, or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

Risk. The likelihood or probability that a loss of information assets or breach of security will occur.

Risk Analysis. The process of evaluating: (a) the vulnerability of information assets to various threats, (b) the costs or impact of potential losses, and (c) the alternative means of removing or limiting risks.

Risk Management. The process of taking actions to avoid risk or reduce risk to acceptable levels.

Sensitive Information. Information maintained by state agencies that requires special precautions to protect it from unauthorized modification, or deletion. See SAM Section 4841.3. Sensitive information may be either public or confidential (as defined above).

User of Information. An individual having specific limited authority from the owner of information to view, change, add to, disseminate or delete such information.

4841.2 INFORMATION INTEGRITY AND SECURITY

Each agency must provide for the integrity and security of its information assets by:

1. Identifying all automated files and databases for which the agency has ownership responsibility (see SAM Section 4841.4);
2. Ensuring that responsibility for each automated file or database is defined with respect to:
 - a. The designated owner of the information within the agency;
 - b. Custodians of information; and
 - c. Users of the information;
 - d. Ensuring that each automated file or database is identified as to its information class (SAM Section 4841.3) in accordance with law and administrative policy;
 - e. Establishing appropriate policies and procedures for preserving the integrity and security of each automated file or database including:
 1. *Agreements with non-state entities to cover, at a minimum, the following:*

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

- a. Appropriate levels of confidentiality for the data based on data classification (see SAM Section 4841.3);*
 - b. Standards for transmission and storage of the data, if applicable;*
 - c. Agreement to comply with all State policy and law regarding use of information resources and data;*
 - d. Signed confidentiality statements;*
 - e. Agreement to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used; and*
 - f. Agreement to notify the State data owners promptly if a security incident involving the data occurs.*
 2. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information and information necessary for the support of agency critical applications;
 3. Auditing usage of dial-up communications and Internet access for security violations;
 4. Periodically changing dial-up access telephone numbers; and
 5. Responding to losses, misuse, or improper dissemination of information.
3. Establishing appropriate departmental policies and procedures to protect and secure IT infrastructure, including:
 - a. Technology upgrade policy, which includes, but is not limited to, operating system upgrades on servers, routers, and firewalls. The policy must address appropriate planning and testing of upgrades, in addition to departmental criteria for deciding which upgrades to apply.
 - b. Security patches and security upgrade policy, which includes, but is not limited to, servers, routers, and firewalls. The policy must address application and testing of the patches and/or security upgrades, in addition to departmental criteria for deciding which patches and security upgrades must be applied, and how quickly.
 - c. Firewall configuration policy, which must require creation and documentation of a baseline configuration for each firewall, updates of the documentation for all authorized changes, and periodic verification of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.
 - d. Server configuration policy, which must clearly address all servers that have any interaction with Internet, extranet, or intranet traffic. The policy must require creation and documentation of a baseline configuration for each server, updates of the documentation for all authorized changes, and periodic checking of the configuration to ensure that it has not changed during software modifications or rebooting of the equipment.

Advance Copy of Changes to State Administrative Manual Sections 4840.4 and 4841.2

- e. Server hardening policy, which must cover all servers throughout the department, not only those that fall within the jurisdiction of the department's IT area. The policy must include the process for making changes based on newly published vulnerability information as it becomes available. Further, the policy must address, and be consistent with, the department's policy for making security upgrades and security patches.

Each state data center must carry out these responsibilities for those automated files and databases for which it has ownership responsibility. See SAM Sections 4841.4 and 4841.5.

Oversight responsibility at the agency level for ensuring the integrity and security of automated files and databases must be vested in the agency Information Security Officer.

The head of each agency is responsible for compliance with the policy described in this section. See SAM Section 4841.1.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 4

Procedures for Unregulated Energy Vendors

**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. 06/01/06)
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 is allowed, but must be pre-approved by CSD.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 5

Procedures for Unregulated Energy Vendors

**ANNUAL 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.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

Attachment 6

Training and Technical Assistance

	NUMBER 07-02
DISTRIBUTION ALL CSD EMPLOYEES	DATE ISSUED March 17th, 2009
SUBJECT COMPUTER SECURITY POLICY	EXPIRES Until amended, superseded, or withdrawn
REFERENCES California Civil Code Section 1798.29 45 C.F.R. Section 160.103 STATE ADMIN. MANUAL (SAM) Section 5300-5399, 8643, 8650, & 8651 Budget Letter BL 05-08 & BL 05-032 Management Memo 06-12 Adm. Serv. Memo #01-06	SUPERSEDES 05-02
INQUIRIES SHOULD BE DIRECT TO: Ed Lee, Chief Information Officer to elee@csd.ca.gov or 916-341-4314	
SIGNATURE: Original is Signed	

This policy is a reference document for employees to be familiar with a number of computer use topics such as Computer Security, Security Training Program, and Computer Safety. Along with providing direction, this policy is intended to instruct managers, supervisors, and employees about their information security responsibilities. Information in this policy is based on security requirements contained in the State Administrative Manual (SAM) Section 5300-5399 on Information Technology.

Included in the Computer Security Policy under Section III is the Computer Security and Confidentiality Statement. When completed, this statement complies with SAM Section 5325, which requires that each employee sign an acknowledgement of their computer security responsibilities. Please complete the following steps:

- * All supervisors and employees will read the Computer Security Policy to understand the Department's computer security policies and practices.
- * All personnel will sign and date the Computer Security and Confidentiality Statement.
- * Supervisors will also sign each form to confirm that all personnel have read and understood the policy.

* All signed certifications will be maintained in the employee's personnel file in the Human Resources Office as documentation of compliance with the Department's policy and SAM Section 5325.

Departmental management is committed to keeping this policy as current as possible. Meeting this goal is a challenge since computer security is a rapidly changing field. If you have any questions or wish to discuss this guide in more detail, please contact the Department's Information Security Officer (ISO).

I. **COMPUTER SECURITY INTRODUCTION**

The Department of Community Services and Development (CSD) has established these policies and procedures to address computer access and data security. CSD employees should adhere to these policies and procedures when accessing automated information systems in their use of computers and related devices. Refer to the Information Technology Section of the State Administrative Manual (SAM) Section 5300-5399 for additional clarification of these security requirements.

A. **OWNERS, CUSTODIANS, AND USERS OF INFORMATION RESOURCES**

The protection of information assets, both paper and electronic format, requires the support and ongoing participation of all owners, custodians, and users of these records. The determination of the custodial and user responsibilities is specific to the information collected, retrieved and/or published for certain audience of viewers.

Owners

Ownership of electronic information resources generally rests with the Department's Information Technology Services Unit. Paper based records ownership falls to the organization originating the document and/or publishing the document. Ownership responsibility for specific data generally rests with the unit management that generates or employs the data. The classification of the information that is entered, processed or distributed is the responsibility of the data owner.

Information access authority should be reviewed on a regular basis, as well as whenever an employee transfers, promotes, separates, or is terminated from state service. Information access authority should be modified or terminated as appropriate.

Custodians

The Information Technology Services Unit staff are the custodians of the information systems and the electronic data for the department. The Local Area Network (LAN) Administrator manages and maintains the LAN environment. The responsibilities of the custodians of information include

the following:

- Comply with all applicable laws, SAM provisions, and CSD policies and procedures.
- Maintain a secure physical and operational environment for storing and processing data resources. Offer support services, information processing services, and technical capabilities, as applicable.
- Advise CSD staff of security vulnerabilities within the system and recommend safeguards.
- Assist in implementing appropriate security precautions.
- Notify the Information Security Officer (ISO) of any actual or attempted security violations and assist in preparing the Security Incident Report (SAM Section 5350) and follow procedures outlined in the CSD Administrative Memorandum 03-01.
- Review information access authority on a regular basis, as well as each time an employee transfers, promotes, separates, or is terminated from state service. Information access authority should be modified or terminated as appropriate.
- Follow appropriate backup and recovery procedures.

Users

Users of information are individuals and state agencies that utilize the information that is processed by automated information systems. Users have specific limited authority from the owner of information to view, change, and/or delete such information.

B. OFF-SITE USAGE

Employees who work from a remote location will exercise the same controls over state-owned electronic and paper data off-site as they do at the Department work site. State-owned data records are considered "confidential" or "sensitive" at the office maintains its classification and access-restrictions off-site. Employees will not permit others access or viewing privileges of such data. Confidential, sensitive and private data releases, which occur by an employee off-site, may result in disciplinary action.

Employees who take state-owned equipment, such as laptop computers LCD projectors off-site and wireless devices, will exercise the same controls over state-owned equipment as they do at the Department work site.

C. CSD INFORMATION SECURITY

The CSD Information Security Officer (ISO) oversees information policies and practices and evaluates the risk management program with respect to information and systems security.

The ISO's responsibilities include the following:

- Oversee agency compliance with policies and procedures regarding the security of information assets (SAM Section 5300.3);
- Review and approval of all Information Security Incident Reports and oversee corrective action to remedy the problem identified (SAM Section 5350);
- Monitor ongoing risk analysis of computer/network applications (SAM Section 5305.1);
- Oversee the development of the Department's Operational Recovery Plan (SAM Section 5355.1);

II. SECURITY TRAINING PROGRAM

The Department has established security measures that recognize requirements of SAM Section 5325. Good security practices are expected of each CSD employee. The following is an overview of good security practices, proprietary software, computer viruses, electronic mail, network information connections, and information security violations which each employee should be aware.

A. GOOD INFORMATION SECURITY PRACTICES

- CSD users accessing CSD information assets must use due care to preserve data integrity and confidentiality.
- Passwords should be treated as confidential information and must be changed on a regular basis so that security, in terms of access, is being maintained.
- CSD users accessing CSD data must take appropriate precautions to ensure the protection of that data from unauthorized access or destruction.
- CSD staff must take reasonable precautions to prevent virus contamination of CSD data files (see section B for further details).
- Use of CSD information assets and computer resources shall be for CSD BUSINESS PURPOSES ONLY.

- Access to the CSD Local Area Network (LAN) system shall be through assigned user identifiers (IDs) and passwords.

B. PROPRIETARY SOFTWARE

Software license agreements shall be strictly followed. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement.

It is the policy of CSD to use commercial software packages for personal computers whenever practical, rather than undertake independent software development.

CSD users may not install freeware or software purchased by them unless the software is approved and added to CSD's supported software list. Unsupported software will be removed.

C. COMPUTER VIRUSES

CSD users must take reasonable precautions to prevent virus contamination of state systems. Caution should be utilized when importing free software from bulletin boards or the Internet. They can be a prime source of computer viruses. No personal or unlicensed software from home and/or from any other source is permitted to be installed in any CSD computer without permission from the Information Technology Services Unit (ITS). In addition, external data or other media files (e.g., jpg, mp3, wma, etc.) may not be used on a CSD computer unless it has been approved by ITSU.

CSD users that access CSD network resources remotely via the GoToMyPC, wireless connections, etc. are responsible for having anti-virus software for any employee owned computers. Users are also responsible for keeping the anti-virus software licensed and up to date.

D. ELECTRONIC MAIL (E-MAIL)

The Department of Community Services and Development (CSD) provides electronic mail (e-mail) services for all staff. This policy applies to all CSD employees and refers to all electronic mail accounts at CSD.

CSD employees who use electronic mail or remotely connects to a CSD email account consent to all of the provisions in this policy and agree to comply with all of its terms and conditions and with all applicable state and federal laws and regulations.

Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

Privacy

CSD cannot guarantee the privacy or confidentiality of any electronic mail message or document. Users should be aware that these transmissions are not secure. Confidential information should not be exchanged via electronic mail without the use of additional security precautions (e.g., encryption, password protected files, etc.).

Proper Use

CSD provides electronic mail service to its employees to enhance their ability to quickly and conveniently send and receive written communications and documents for the purpose of conducting state business. Any use of this service that interferes with these functions is improper.

Employees who use the electronic mail service are expected to do so responsibly, to comply with state and federal laws, with policies and procedures of the department, and with normal standards of professional and personal courtesy and conduct. For example, an e-mail message that will be sent to all CSD staff or to Executive Staff should be reviewed and approved by the sender's supervisor/manager, as would a hard copy memo being sent to these recipients. The same reporting lines should apply as appropriate (from staff to supervisor, to manager, to deputy director, to chief deputy director, to director).

Other considerations should include the urgency of the message, the length of the message, and the nature of the message. E-mail messages normally involve short, concise, communications about very current or urgent business matters. Lengthy documents and purely informational material are better shared through the CSD Intranet or shared via regular internal office mail system. An exception would be a document being e-mailed to your supervisor for editing.

The nature of the message is also important. E-mail communications are not intended to take the place of interpersonal verbal communication that is necessary and appropriate to conduct business. CSD expects its employees to exercise good judgment in deciding which matters are communicated by e-mail rather than by telephone or in person. For example, sensitive personnel issues are not appropriately conducted or resolved by electronic communication. Questions about these distinctions should be directed to the employee's supervisor/manager or to the Deputy Director for Administrative Services.

As the owner of the electronic mail system, CSD reserves the right to monitor and inspect electronic mail transmissions for reasonable business purposes. *Electronic mail may only be used for legitimate state business purposes.*

Improper Use

Electronic mail transmission must not be used to contact others for commercial ventures, religious or political causes, or other non-business purposes such as "junk mail", jokes, or chain letters.

CSD strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, CSD prohibits the use of the electronic mail service in ways that are disruptive, offensive to others, harmful to morale, or discredit and/or reflect poorly on CSD in any way.

- *Example: The display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.*

In general, policies and regulations that apply to other forms of communication at CSD also apply to electronic mail. For example, it is CSD's policy that personal information about an employee, such as illness or a death in the family, should not be shared with other staff or the entire staff until the employee has agreed with his/her supervisor to share the information. The employee's manager should issue any electronic mail messages about such personal matters.

In addition, the following specific actions and uses of electronic mail are improper:

- Concealment or misrepresentation of names or affiliations in electronic mail messages.
- Alteration of source or destination addresses of electronic mail.
- Use of electronic mail to aid in unlawful activities.
- Use of electronic mail for commercial or private business purposes.
- Use of electronic mail, which unreasonably interferes with or threatens other individuals.
- Use of electronic mail that degrades or demeans other individuals.

CSD electronic mail service shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing or networking facility, or unwarranted or unsolicited interference with others' use of electronic mail. These uses include but are not limited to:

- sending and/or forwarding chain letters;
- "letter bombs" or sending the same electronic mail message repeatedly to one or more recipients to interfere with the recipient's use of electronic mail; and

- to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic mail.

Employees should notify their immediate supervisor, the Information Security Officer, or any other member of management upon learning of a violation of this policy.

Security

All users of electronic mail are advised to take necessary precautions to protect the confidentiality of electronic mail messages and documents or other records containing personal or confidential information encountered in the performance of their duties or otherwise. They should therefore utilize whatever means of protection, such as passwords, that are available to them to safeguard their electronic mail. Since such means of protection are not necessarily foolproof, the security and confidentiality of electronic mail cannot be guaranteed.

E. LOCAL AREA NETWORK

- Groups in the shared folders are established and maintained by the Network Administrator.
- To establish a new group or to modify an existing group requires a request to be submitted to the Product Specialist.
- Because shared files can only be opened by one person at a time, files should not be left open when you are going to be away from your computer for 15 minutes or longer (i.e., breaks, attending meetings, having lunch).
- The user will be responsible for "managing" the files stored in the user's network folder (i.e., removing inactive/duplicate files).
- The user will be responsible to logout of their network account each evening prior to departure from CSD nor will any employee maintain an active remote connection when not necessary.

F. INFORMATION SECURITY VIOLATIONS

The ISO, with full departmental support and authority, will treat violations of security policy with the utmost seriousness. In the course of enforcing this Department's information security policies and procedures, the ISO may recommend taking disciplinary action. The specific disciplinary action that will be taken depends upon the nature of the violation and the impact on the Department's information assets and/or facilities. Disciplinary action may include:

- A written letter of reprimand;
- Time off without pay;
- Reduction in pay;
- Demotion;
- Dismissal from state service;
- Criminal prosecution.

Follow-up and resolution of reported security incidents will be prompt. During the time when a suspected violation is under investigation, the suspected violator's access privileges may be revoked and/or other action may be taken to prevent harm to CSD's information assets. Depending on the infraction, a Security Incident Report may be required as described above.

III. COMPUTER SAFETY

Steps should be taken to protect computer equipment from theft and unauthorized use. Desktop systems should be kept in secure areas or should be physically attached to a desk or table. The following is an overview of the CSD computer safety policies and procedures.

A. BACKUP/RECOVERY PROCEDURES AND OFF-SITE STORAGE

To guard against the loss of data and programs and to ensure the availability and integrity of application software and data, the Information Technology Services Unit will maintain back-up copies of all programs and data on the LAN according to the following guidelines:

- A regular schedule for making backup copies of all data files shall be established by the Information Technology Services staff.
- Unit management, in coordination with the ISO, will ensure that backup procedures are carried out.
- Depending on the nature of the information, backup files may need to be stored at an off-site location.
- If software cannot be copied to make backups (because of copy protection or legal restrictions), enough information must be retained to allow an identical copy to be obtained if necessary.
- To ensure that data/documents are backed up, all files should be

saved on the LAN. Files saved on the local workstations are the responsibility of the end user.

B. PASSWORD PROTECTION (Securing the Data from Unauthorized Access)

CSD employees are responsible for the confidentiality and security of their passwords. **Shared passwords are prohibited.** To protect the Department's LAN resources, either password protect your screen saver or log off the computer when your workstation is unattended.

- Logon ID's are limited to 11 (eleven) characters, with no minimums.
- The first time a user logs on to their computer, the LAN administrator will assign the password. The user will then be prompted to change their password ID.
- Passwords must be at least six (6) characters long, and are case sensitive.
- If a password is forgotten, a request must be submitted to the Product Specialist.
- Passwords are good for 60 days. At the end of 60 days the password must be changed. The same password cannot be used twice.

C. FILE ENCRYPTION (Securing the Data from Accidental or Unauthorized Access)

Confidential data files should be protected from unauthorized access or modification through data encryption.

D. RISK MANAGEMENT PROGRAM - Operational Recovery Planning (ORP)

A risk management program includes a contingency plan that addresses what to do if, and when, your computer and/or the data files are violated, lost, damaged, or inaccessible. Other terms for contingency plan are Disaster Recovery Plan or Operational Recovery Plan (ORP). The ORP contains detailed procedures that will help assure continued agency operations in the event of a disaster (SAM Section 5355). The ORP is part of the Department's overall Business Recovery Plan. Responsibility for preparing and updating the ORP resides with the management of each program. The ORP is a tool to the program management to recover its information assets in the event of a major disaster.

COMPUTER SECURITY AND CONFIDENTIALITY STATEMENT

I have read the Computer Security Policy Guide and will comply with the security requirements indicated in the guide. Also, I understand the need to:

1. Exercise due care to preserve data integrity and confidentiality.
2. Treat passwords as confidential information and change them on a regular basis to help ensure that security is maintained.
3. Take reasonable precautions to ensure the protection of CSD data from unauthorized access or destruction.
4. Notify my supervisor and the CSD Information Security Officer when aware of a possible security violation including unauthorized access, loss or destruction of equipment, misuse, theft, possible virus, etc. (see Section 5350 of the State Administrative Manual).
5. Re-certify by completing this form annually.

CERTIFICATION

I understand that unauthorized access, attempted access, or use of any computer systems and/or data of the State of California is a violation of Section 502, of the California Penal Code, and is subject to prosecution.

_____	_____	_____
User name (print)	Division	Unit
_____	_____	_____
User signature	Date	Telephone number
_____	_____	_____
Supervisor signature	Date	Telephone number

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

2011 LIHEAP Contract

Page A3

Page C1

Pages D5

**EXHIBIT A
(Standard Agreement)**

- B. Notice shall contain a statement of the reasons for termination with reference to the specific provision(s) in the grant guidance or proposed amendment in question.
- C. Contractor shall be entitled to reimbursement for all allowable costs incurred prior to termination of the contract. Such reimbursement shall be in accordance with the grant guidance and contract provisions in effect at the time the cost was incurred.

6. COMPLIANCE

All services and activities are to be provided in accordance with all applicable federal, state, and local laws and regulations, and as those laws and regulations may be amended from time to time, including but not limited to, pursuant to the following:

- A. The Low-Income Home Energy Assistance Program Act of 1981, 42 U.S.C. §§ 8621 et seq., and 45 Code of Federal Regulation (CFR) Part 96;
- B. The California Government Code §§ 16367.5 et seq., as amended, and Title 22, California Code of Regulations (CCR), §§ 100800 et seq.; and
- C. The Single Audit Act, 31 U.S.C. §§ 7301 et seq., and Office of Management and Budget (OMB) Circular A-133 and its appendices and supplements.

7. REQUIREMENTS, STANDARDS, AND GUIDELINES

Contractor agrees to apply all of the requirements, standards, and guidelines contained in the following authorities, as they may be amended from time to time, to all of the procurement, administrative, and other costs claimed under this Agreement, including those costs under subcontracts to this Agreement, notwithstanding any language contained in the following authorities that might otherwise exempt Contractor from their applicability. To the extent that the requirements, standards, or guidelines directly conflict with any State law or regulation at Government Code §§ 16367.5 et seq. or 22 CCR §§ 100800 et seq., or any specific provision of this Agreement, then that law or regulation or provision shall apply instead:

- A. OMB Circular A-102 (Common Rule for State and Local Governments), as codified by the Department of Health and Human Services (HHS) at 45 CFR Part 92;
- B. OMB Circular A-110 (Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals and other Non-Profit Organizations), as codified by HHS at 45 CFR Part 74;

EXHIBIT C
(Standard Agreement)

GENERAL TERMS AND CONDITIONS GTC 610

1. APPROVAL

This Agreement is of no force or effect until signed by both parties.

2. AMENDMENT

No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or Agreement not incorporated in the Agreement is binding on any of the parties.

3. ASSIGNMENT

This Agreement is not assignable by the Contractor, either in whole or in part, without the consent of the State in the form of a formal written amendment.

4. AUDIT

Contractor agrees that the awarding department, the Department of General Services, the Bureau of State Audits, or their designated representative shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (Gov. Code § 8546.7, Pub. Contract Code § 10115 et seq., CCR Title 2, Section 1896.)

5. INDEMNIFICATION

Contractor agrees to indemnify, defend and save harmless the State, its officers, agents and employees from any and all claims and losses accruing or resulting to any and all contractors, subcontractors, suppliers, laborers, and any other person, firm or corporation furnishing or supplying work services, materials, or supplies in connection with the performance of this Agreement, and from any and all claims and losses accruing or resulting to any person, firm or corporation who may be injured or damaged by Contractor in the performance of this Agreement.

EXHIBIT D
(Standard Agreement)

- E. If the Contractor's board is both tripartite and advisory to the elected members governing a local government, the Contractor shall submit to CSD the approved minutes from any meeting of the elected officials where matters relating to this Agreement are heard, including but not limited to discussions about or decisions affecting the Low-Income Home Energy Assistance Program. Such minutes shall be submitted to CSD no later than 30 days after the related meeting.

6. AUDITING STANDARDS AND REPORTS

A. Auditing Standards

Contractor must follow all audit requirements as set forth in OMB Circular A-133 and the CSD Supplemental Audit Guide. The Supplemental Audit Guide is attached herein as Exhibit D, Attachment I. The Supplemental Audit Guide may be accessed at www.csd.ca.gov.

B. Audit Reports

- 1)
 - a. Funds provided under this Agreement shall be included in an audit conducted in accordance with the provisions of OMB Circular A-133 for nonprofit and public agencies; standards promulgated by the American Institute of Certified Public Accountants (AICPA), and those standards included in "Government Auditing Standards, 2007 Revision, as amended."
 - b. Contractors falling below the federal funding threshold that mandates a single agency-wide audit in accordance with OMB Circular A-133 shall:
 - i. Submit an annual program-specific audit within nine months of the end of the Contractor's fiscal year; and
 - ii. Be subject to an audit and/or other fiscal- or program-specific review conducted by CSD or its agents, upon 30 days written notice.
- 2) The financial and compliance audit report shall contain the following supplementary financial information: a combined statement of revenue and expenditures for each contract that presents, by budget line item, revenue and expenditures for the audit period and a description of the methodology used to allocate and claim indirect costs and any administrative cost pools.
- 3) The audit report must specifically mention that a review for compliance with OMB Circulars A-87 and A-122 was conducted.

PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT

LIHEAP Verification

And

Eligibility Guide

Pages 9-11

Pages 20-45

Citizenship and Alien Status for Public Agencies

Purpose Federal law requires that all public agencies verify that all eligible applicants are a United States citizen, national, or an alien in a qualified immigration status.

Citizen or naturalized citizen An individual is a United States (U.S.) citizen if:

- Born in the U.S., regardless of the citizenship of his/her parents
- Born outside of the U.S. of U.S. citizen parents
- Born outside the U. S. of alien parents and has been naturalized as a U.S. citizen. A child born outside of the U.S. of alien parents automatically becomes a citizen after birth if his/her parents are naturalized before he becomes age 16.

Citizenship documentation Acceptable proof of U.S. citizenship includes but not limited to:

- U.S. birth certificate
- U.S. passport
- Naturalization certificate, N-550 or N-570. Certificate cannot be copied but agency should review, verify and document in the file that the “naturalized certificate was verified and valid”
- Report of birth abroad of a U.S. Citizen FS-240
- United States Citizen Identification Card, I-197
- Certificate of Citizenship, N-560 or N-561
- Statement provided by the U.S. consular officer certifying the individual is a U.S. citizen
- American Indian card with a classification code KIC

Qualified Alien The following table lists acceptable status and corresponding documentation for qualified aliens:

Status	Documentation
Lawful Permanent Resident	<ul style="list-style-type: none"> • INS form I-551 (Alien Registration Receipt Card, also called Resident Alien Card or ‘green card’). This card contains a photo and fingerprint. It does not include the AI-551 form number. Older versions do not include a fingerprint. • An unexpired temporary I-551 stamp in a foreign passport or on a Form I-94

Continued on next page

Citizenship and Alien Status for Public Agencies, Continued

Qualified Alien
(continued)

Status	Documentation
Parolee	<ul style="list-style-type: none"> • INS Form I-94 with a stamp showing admission under Section 212(d)(5) of the INA. An expiration date of 1 year or more from the date the status was granted (or indefinite) will be noted on the I-94 and can be used to indicate a qualified alien's status • INS Forms I-688 coded 274a.12(c) (11) • Form I-766 coded C11, indicates parolee status
Conditional Entrant	<ul style="list-style-type: none"> • INS Form I-94 with a stamp showing admission under Section 203(a)(7) of the INA • INS Form I-688 coded 274a.12(a)(3) • Form I-766 coded A3, which indicates status as a condition entrant
Cuban/Haitian Entrant	<ul style="list-style-type: none"> • INS Form I-94 with a stamp showing parole as a Cuban/Haiti Entrant under Section 212(d)(5) of the INA • Form I-94 showing parole into the U.S. on or after October 10, 1980 and reasonable evidence that the parolee had been a national of Cuba or Haiti • Note: This guideline does not apply when the individual was paroled solely to testify as a witness in a judicial administrative, or legislative proceeding or when the parolee is in legal custody pending criminal prosecution
Deportation or Removal Withheld	<ul style="list-style-type: none"> • An immigration judge's order showing that deportation was withheld pursuant to Section 243(h) of the INA removal was withdrawn pursuant to Section 241(b)(3) of the INA and the date of the judge's order • An INS Form I-688 with the code of 274a.12(a)(10) • Form I-766 coded A10, which indicates deportation or removal withheld under Section 241(b)(3) or 243(h)
Battered Spouse	<ul style="list-style-type: none"> • The individual must have filed a petition with INS base on: <ul style="list-style-type: none"> Status as a spouse or child of a United States citizen or classification to immigrant status as a spouse or child of a lawful permanent resident or Suspension of deportation and adjustment to lawful permanent resident status based on battery or extreme cruelty by a spouse or parent who is a United States Citizen or lawful permanent resident • The individual must allege that he or she was subjected to battering or extreme cruelty; and the person responsible for the battery or extreme cruelty must no longer reside with the individual in question.

Continued on next page

Citizenship and Alien Status for Public Agencies, Continued

Qualified Alien (continued)

Status	Documentation
Asylee-Alien granted asylum	<ul style="list-style-type: none"> • INS Form I-94 (Arrival Departure Record) with a stamp showing grant of asylum under Section 208 of the INA • A grant letter from the INS Asylum Office. • An order of an immigration judge. • INS Form I-688B (Employment Authorization Card) with the code 274a.12(a)(5) • Form I-766 (Employment Authorization Document) coded A5 that indicates status as an Asylee
Refugee	<ul style="list-style-type: none"> • INS Form I-94 with a stamp showing admission under Section 207 of the INA • INS Form I-688B with the code 274a.12(a)(3). • Form I-766 coded A3 that indicates status as a refugee.

Ineligible for public agencies

Persons ineligible to participate in the energy and/or weatherization programs with public agencies are:

- Individuals who hold an INS I-94 who are admitted as temporary entrants (such as students, visitors, tourists, diplomats, etc.)
- Aliens who have no other INS document
- Individuals possessing an Individual Taxpayer Identification Number (ITIN). An ITIN does not create an inference regarding the person's immigration status. An ITIN is issued by the U.S. Internal Revenue Service to individuals who are required to have a U.S. taxpayer identification number but who do not have, and are not eligible to obtain a Social Security Number issued by the Social Security Administration.

Calculating income

An individual is not counted in the household size if citizenship or qualified alien criteria is not met. However, his/her income is counted in the household's total income.

Processing Applications without a Social Security Number

Background

CSD does not have the legal authority to require the collection of Social Security numbers (SSN) as a condition of eligibility. Agencies should continue to request an SSN to assist with client identification and to streamline applicant eligibility verification. However, an applicant cannot be denied services for refusing to provide their Social Security number.

Mail in applications

If an application is received in the mail without an SSN, the agency must follow up with the client to request the SSN. If the client refuses to submit the SSN the agency must follow the step by step procedure for processing an application without an SSN as described on page 21.

The attempt to obtain the SSN and the reason for not providing the SSN by the client must be documented in the client file.

Applications received in person

If during the initial intake process an application is submitted without an SSN and a verbal confirmation is received from the client that they refuse to provide their SSN, the agency will follow the step by step procedure for processing an application without an SSN as described on page 21.

The attempt to obtain the SSN and the reason for not providing the SSN by the client must be documented in the client file.

Requesting additional information

Note: Agencies that require documentation above the minimum requirements (a copy of Social Security card, copy of a driver's license, or name, ages and Social Security numbers for all household members) cannot deny a client for services for failure to provide this additional information.

Continued on next page

Processing Applications without a Social Security Number

Continued

Procedure

If a client refuses to provide their SSN:

Step	Action
1	Agency must confirm identity of client with any picture identification card. A copy of the picture identification used to confirm identity must be retained in the client file. Examples of acceptable forms of picture identification: <ul style="list-style-type: none"> • Drivers license • Employee ID card • School, library, bus pass etc.
2	After confirming the applicant's identity, perform a data base search using the following information to assure that the client has not been served in the current program year: <ol style="list-style-type: none"> 1. Last and first name 2. Service address 3. Phone number 4. Utility Account Number
3	If the client's record is located in a prior year with an SSN, agencies can enter the application and use the SSN from the prior year on the current application. The application should be processed in the standard manner and will not need to be submitted to CSD.
4	When the client is determined eligible (meets income guidelines, agency's priority plan and has not been served in the current year) agency will arrange for the handling of the application without an SSN, by completing a fax coversheet, and submitting the cover sheet, a copy of the intake form and supporting documents to CSD's Help Desk, via fax. Supporting documents must include: <ol style="list-style-type: none"> 1. Utility bill or a landlord statement for utilities included in rent 2. Copy of picture ID
5	CSD's Help Desk staff will perform a secondary duplicate check to confirm the client has not previously applied with an SSN. If a positive match is found, the Help Desk will provide the agency the previously used SSN for processing of the application.
6	If no match is found a unique filler number will be assigned by the Help Desk in lieu of an SSN.
7	Help Desk will confirm the filler number assigned to the applicant and provide the agency the temporary SSN via the return of the completed fax cover sheet.
8	Once the agency receives the confirmation with the assigned filler number the agency will process the application in the standard manner. <p>Note: Once an applicant is assigned a temporary filler number, this number is to be used each and every year the client applies.</p>

Client File Documentation

Purpose All factors of eligibility must be verified and documented in the client file.

Client file requirements Client files must contain specific documents:

1. Completed and signed intake form. The applicant name and signature must be the same person. Note: The applicant does not need to be the customer on the utility bill.
2. Copy of the utility bill from the company that will receive the cash assistance (HEAP) payment. It is important to collect bills from all sources of energy used in the household to determine the actual energy burden. However, copies of all sources are not required.
3. Proof of income documentation for all adult members of the household for a one month period, current within six weeks of intake.
4. Verification of energy conservation education and budget counseling.
5. If the agency is required to verify citizenship, the file must contain proof as directed.

Fast Track requirements Fast Track client files must contain all of the requirements listed in the previous section and proof of energy crisis documentation, such as:

- A shut off notice,
- Proof that services have been disconnected,
- Proof that the account is in arrears, or
- A deposit is needed to establish services

Not required by CSD CSD does not require a copy of the applicant's

- Social Security card
- Drivers License
- Name, age, and social security number for all members of household

It is at the agency's discretion to include these documents in the client file.

Confidential Agency personnel will be exposed to and have access to information which is of a confidential nature. All client records are considered to be confidential and are open only to State and local agency personnel carrying out eligibility and audit functions. Such information should not be shared with unauthorized personnel.

Retention All client files must be retained for 3 years from the end of the contract term.

Income Verification

Introduction

The determination of income is based on all household income sources before any deductions. An applicant's total gross household income must be verified and copies retained in the client file.

Income Calculation

Introduction Determination of income eligibility is based on the total household monthly gross income before any deductions. Applicants are required to submit proof to cover one month's income.

Purpose To create consistency in calculating income, agencies must calculate monthly income using the same method. The income calculations is to assist clients experiencing hardships and not be used as a common practice to circumvent the requirements for collecting income documentation substantiating gross monthly income from all sources for qualified households.

- Criteria**
- Proof of income must be current to within 6 weeks from the intake date (unless otherwise specified by the agency).
 - Income must be the total gross income before deductions.
 - Income document(s) should cover a one-month period unless applicant did not work a full month.
 - Income cannot be annualized.
 - Seasonal worker's income must be based on the actual current income at time of intake.
-

Total income submitted When four weekly, two bi-weekly or two bi-monthly consecutive paystubs are submitted as proof, simply add the gross amount of all stubs to calculate monthly income.

Exceptions On an exceptional basis when a client cannot provide a full month of income verification, a weekly, bi-weekly or bi-monthly paycheck stub can be used to equal one month income using the income formulas in the following section. However, income formulas cannot be used when the calculated monthly income does not reconcile (within reason) with client's statement of gross monthly income or if the client failed to provide a statement of their gross monthly income on the intake form. The applicant must first state the amount of their gross monthly income on the intake form; and then proceed to provide the proof.

Example A

Stated Income on Intake Form:	\$800
Weekly Pay Stub:	\$200
Income using formula (\$200 X 4.333)	\$866.60

Example A is an acceptable method for utilizing the income formula for determining monthly income as the monthly calculated income reconciles within reason with the client's statement of gross monthly income on intake form. In this example the total household income entered would be \$866.66.

Example B

Stated Income on Intake Form: \$0
Weekly Pay Stub: \$200

Example B is an unacceptable situation to allow the utilization of the income formula for determining client's monthly income. The proof of income provided does not reconcile against the income stated on the intake form. The applicant must declare their monthly income.

Income Formulas

How to calculate incomplete earned income documentation

- A weekly gross income must be multiplied by 4.333 to total one month's income.
 $\$550 \text{ weekly} \times 4.333 = \$2,383.15 \text{ monthly income}$
- Bi-weekly gross income should be multiplied by 2.167 to calculate one month's income.
 $\$1,200 \text{ bi-weekly} \times 2.167 = \$2,600.40 \text{ monthly income}$
- Bi-monthly gross income should be multiplied by 2
 $\$1,200 \text{ bi-monthly} \times 2 = \$2,400.00 \text{ monthly income}$
- Quarterly gross income (including any interest and dividends) should be divided by 3 to arrive at a monthly average.
 $\$4,000 \text{ quarterly divided by } 3 = \$1333.33 \text{ monthly income}$

Note: The income calculation is to assist clients experiencing hardships and not be used as a common practice to circumvent the requirements for collecting income documentation substantiating gross monthly income from all sources for qualified households.

Zero Income

For clients claiming no source of income, verification must be certified by completing a self-certification statement or use CSD Form 43A. The statement must include the individual's name, date, signature, and attest to the fact that all statements are true and correct.

Statement of income

In all cases agencies should make every effort to obtain one month's income documentation from all income sources. The first step is to verify the amount of the household's gross monthly income, generally provided on the intake form, along with the provided acceptable forms of income verification to substantiate the amount indicated on the intake form.

If the client has not indicated the monthly amount and is available, simply ask them to enter it on the form. If an intake form is received by mail without the income box completed, a second attempt to obtain the information must be made, either by mail, phone call, fax, etc. In all cases, the attempt to obtain the monthly income amount and verification as well as any subsequent actions must be documented in the client file.

If it is determined that a hardship exists and the client is unable to provide verification after the agency has made an attempt to obtain documentation, it is then acceptable to process the application using the formulas for calculating incomplete earned income.

Public assistance, retirement, Social Security

Clients should be expected to provide appropriate verification for one entire month. The only exception would be when the request for additional documentation would cause undue hardship for the client and the income can be substantiated with a great deal of accuracy using an outdated form of documentation.

Example: Elderly woman, 80 years old, using public transportation to the agency, submits a copy of a Social Security check that is beyond the 6 week limit. It is reasonable, in this case, to assume that her income, Social Security, has not changed and it is acceptable to process the application with the income verification submitted. It would be an extreme hardship for the applicant to return with current documentation.

Note: The reason for accepting the outdated information must be documented in the file.

Unqualified alien

An individual that is not a citizen or a qualified alien is not counted in the HEAP household. However, his /her income is counted towards the household's total income.

Annual statements and bank deposits

For award or annual statements, DO NOT use the date the document was issued. You must use the dates covering benefits within the document to determine eligibility. These dates must be current.

Automatic Bank Deposit - the date of the deposit or the issue date of the statement can be used to determine if the document is current to within 6 weeks of intake date.

Acceptable & Excluded Income Documentation

Public Assistance

Definition Public assistance or welfare payments include cash public assistance payments low-income people receive, such as aid to families with dependent children (AFDC, ADC), temporary assistance to needy families (TANF), and general assistance.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of current check
- Current Notice of Action
- Current verification from worker with amount of payment and date
- Food Stamp verification with current income amount listed
- Current aid printout summary
- Copy of bank statement showing direct deposit; the date of the deposit or the issue date of the statement can be used to determine if the document is current to within 6 weeks of intake date.

Unacceptable proof

- Outdated or altered information
- Medi-Cal cards
- Food Stamp verification with no income amount or date
- CW7 Report
- Notice of Action stating homeless aid

Countable income Overpayment adjustments should not be deducted from the grant amount.

Non-countable income A family's monthly Food Stamp allotment amount is not considered income.
Note: Do not include the Food Stamp amount when calculating income

Earned Income

Definition

Money, wage or salary income is the total income people receive for work performed as an employee during the income year. Includes wages, salary, armed forces pay, commissions, tips, piece-rate payments, and cash bonuses earned, before deductions are made for items such as taxes, bonds, pensions, and union dues.

Acceptable proof

Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of check(s) showing gross amount.
 - Current copy of pay stub(s) covering 1 month of gross income (using necessary formulas).
 - Letter from employer with company name, address, phone number, the gross amount and current pay period.
 - Notice of Action showing earned income.
 - HUD statement from Department of Housing with annual income amount.
-

Unacceptable proof

- Outdated information
 - Information without dates
 - Copy of check(s) showing net amount only
 - Federal and State Tax Forms (exception: self-employed)
 - W2 Forms
 - Non-consecutive pay stubs (If unable to determine monthly gross.)
 - Employers' letter not showing gross income amount
 - Food Stamp verification with no dollar amount listed
 - Renter's Credit Form
 - Copy of bank statement
 - Military pay showing base pay only.
-

Social Security

Definition Includes social security pensions and survivor's benefits and permanent disability insurance payments made by the SSA prior to deductions for medical insurance.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of check
- Payee's (income recipient) letter of verification showing income amount
- Notice of planned action
- Copy of bank statement showing direct deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

For the following items, DO NOT use the actual date the document was issued. You must use the dates covering benefits within the document to determine eligibility. These dates must be current.

- Annual benefit letter with current dates (i.e., date of letter is 12/08, but letter states applicant will receive \$\$ beginning 1/09).
- Computer printout or letter that states the current annual benefit amount.
- Form 2458 completed by Social Security Office.
- HUD statement from Department of Housing with a Social Security amount.

Unacceptable proof

- Outdated information
- Benefit letter with no income amount or date
- Payee's letter of verification not showing income amount
- Medicare cards

Countable income Overpayment adjustments must not be deducted.

Continued on next page

Social Security, Continued

**Non-countable
income**

Medicare premiums are not considered income and must be deducted from the total gross amount.

Pensions or Retirement

Definition Includes payments received from eight sources: companies or unions; federal government (Civil Service); military; state or local governments; railroad retirement; annuities or paid-up insurance policies; individual retirement accounts (IRAs), Keogh or 401 (k) payments; or other retirement income.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of check.
- Copy of bank statement showing direct deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

For award or annual statements, DO NOT use the date the document was issued. You must use the dates covering benefits within the document to determine eligibility. These dates must be current to within 6 weeks of the application intake date.

- Pension verification (i.e., letter or printout. Time frame of benefit must be current).
 - Annual statement from pension plan.
 - Form 1099. (Only acceptable if intake date is within the 6 week period following January 1, 2009.)
-

Unacceptable proof

- Outdated or altered information
- Benefit letter with no income amount or date

Interest

Definition Interest includes payments received or have credited to accounts from bonds, treasury notes, IRAs, certificates of deposit, interest-bearing savings and checking accounts, and all other investments that pay interest. Only the interest used for household support is considered income, not the original deposit.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Current copy of check(s)
- Current statement(s) from financial institution(s)
- Current copy of financial statement(s) showing direct deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date

Unacceptable proof

- Outdated information
- Information without a date
- Financial statement(s) without a dollar amount listed
- Federal and State Tax Forms

Dividends/Royalties

Definition Dividends are returns on capital investments, such as stocks, bonds, or savings accounts. Royalties are compensation paid to the owner for the use of property, usually copyrighted material or natural resources such as mines, oil wells, or timber tracts. Royalty compensation may be expressed as a percentage of receipts from using the property or as an amount per unit produced.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Current copy of check(s)
- Current statement(s) from financial institution(s)
- Current copy of financial statement(s) showing direct deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

Unacceptable proof

- Outdated information
- Information without a date
- Financial statement(s) without a dollar amount listed
- Federal and State Tax Forms

Workers Compensation

Definition Workers compensation includes payments people receive periodically from public or private insurance companies for injuries received at work.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of current check(s)
 - Current check stub(s)
 - Current printout
 - Current award letter
-

Unacceptable proof

- Outdated information
 - Information without a date
 - Award letter without income or date
-

Unemployment Compensation

Definition Unemployment compensation includes payments received from government unemployment agencies or private companies during periods of unemployment, including any strike benefits from union funds.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of current check(s)
 - Current check stub(s)
 - Current printout
 - Current award letter
-

Unacceptable proof

- Outdated information
 - Information without a date
 - Award letter without income or date
-

Veterans Benefits

Definition Includes payments to disabled members of the armed forces or survivors of deceased veterans receiving periodically from the Department of Veterans Affairs for education and on-the-job training, and means-tested assistance to veterans.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of current check(s)
- Current check stub(s)
- Current printout
- Current award letter
- Bank statement with automatic deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

Unacceptable proof

- Outdated or altered information
- Benefit letter with no income amount or date

Self Employment and Rental Income

Definition

Net earnings from self-employment are the gross income from any trade or operated business minus any allowable deductions for that trade or business. Net earnings also include the client's share of profit or loss in any partnership, as reported on Federal income tax returns.

Operational expenses for self employed

The following are operational expenses for self employed and are not considered income:

- Taxes required for operation of the business
 - Licenses and permit fees
 - Rent payments
 - Insurance
 - Labor costs
 - Maintenance
 - Products used to operate the business
 - Interest on debts
 - Actual food costs for self employed babysitters
-

Not included in operational expenses

Business expenses do not include:

- Payments on the principal of the purchase price of and loans for capital assets such as real property, equipment, machinery and other goods of durable nature
 - The principal and interest on loans for capital improvement of real property
 - Net losses from previous periods
 - Federal, state, and local taxes
 - Money set aside for retirement purposes
 - Personal expenses, entertainment expenses, and personal transportation
 - Depreciation on equipment, machinery, or other capital investments necessary to the self-employment enterprise
-

Continued on next page

Self Employment and Rental Income, Continued

Operational expenses for rentals

The following are operational expenses for rentals and are not considered income:

- Interest on debts
 - Taxes
 - Insurance
 - Maintenance
 - Utilities, if paid by applicant
 - Real estate agent's fees
-

Acceptable proof

Tax Form 1040 is acceptable until the following year's filing date. The 2009 Income Tax Form is good until April 15, 2010.

- Current signed 1040 Federal Tax Form.
Must show a dollar amount, either on line 12 or 17, to be valid income verification for self-employed. When using a 1040 Tax Form, calculate monthly gross income for self-employed by dividing the amount on line 22 by 12 months. If line 22 is zero or a negative amount, set the income amount on the application to zero (0).
 - Current copy of ledger or journal (Handwritten information is acceptable) - Proof of income for a copy of ledger or journal, or a self-employment statement must be current to within 6 weeks of the application intake date.
 - Signed self-employment statement showing gross receipts, gross expenses, and net income for a one month time period (within the last six weeks).
-

Unacceptable proof

- Outdated or altered information.
- Unsigned 1040 Federal Income Tax Form

Survivors Benefits

Definition Survivors benefits include payments received from survivors' or widows' pensions, estates, trusts, annuities, or any other types of survivor benefits, from private companies or unions; federal government (Civil Service); military; state or local governments; rail road retirement; worker's compensation; black lung payments; estates and trusts; annuities or paid-up insurance policies; and other survivors benefits.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of current check(s)
- Current check stub(s)
- Current printout
- Current award letter
- Bank statement with automatic deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

Unacceptable proof

- Outdated information
- Information without a date
- Award letter without income or date

SSI/SSP

Definition Supplemental security income includes federal, state, and local welfare agency payments to low-income people who are 65 years of age and older or people of any age who are blind or disabled.

Acceptable proof Proof of income for these items must be current to within 6 weeks of the application intake date.

- Copy of check
- Payee's (income recipient) letter of verification showing income amount
- Notice of Planned Action
- Copy of bank statement showing direct deposit - The date of the deposit or the issue date of the statement can be used to determine whether the document is current to within 6 weeks of intake date.

For the following items, DO NOT use the actual date the document was issued. You must use the dates covering benefits within the document to determine eligibility. These dates must be current.

- Annual benefit letter with current dates (i.e., date of letter is 12/08, but letter states applicant will receive \$\$ beginning 1/09).
 - Computer printout or letter that states the current annual benefit amount.
 - Form 2458 completed by Social Security Office.
 - HUD statement from Department of Housing with a Social Security amount
-

Unacceptable proof

- Outdated information
- Benefit letter with no income amount or date
- Payee's letter of verification not showing income amount
- Medicare cards

Countable income Over payment adjustments must not be deducted.

Non-countable income Medicare premiums are not considered income and must be deducted from the total gross amount.

Excluded Income Sources

Policy change Effective with the release of the DOE ARRA contracts, the criteria for countable and non-countable income is being updated to include the following exclusions.

Authority **Federal Law Title 42 Chapter 94**
In verifying income eligibility for purposes of subsection (b) (2) (B) of this section, the State may apply procedures and policies consistent with procedures and policies used by the State agency administering programs under part A of title IV of the Social Security Act [42 U.S.C. 601 et seq.], under title XX of the Social Security Act [42 U.S.C. 1397 et seq.], under subtitle B of title VI of this Act (relating to community services block grant program) [42 U.S.C. 9901 et seq.], under any other provision of law which carries out programs which were administered under the Economic Opportunity Act of 1964 [42 U.S.C. 2701 et seq.] before August 13, 1981, or under other income assistance or service programs (as determined by the State).
Subsection (b) (2) (B) households with incomes which do not exceed the greater of- (i) an amount equal to 150 percent of poverty level for such state; or (ii) an amount equal to 60 percent of the State median income;

Student Assistance All student assistance is excluded. This includes Grants, Scholarships, Fellowships and Gifts/Pell Grants/Federal Perkins Loans, Federal Supplemental Education Opportunity Grants, Leveraging Educational Assistance Program (LEAP), Department of Education and Bureau of Indian Affairs (BIA), University Year for Action and work study.

Foster Care payments Payments received for the care of foster children or foster adults, who are unable to live alone.

Continued on next page

Excluded Income Sources, Continued

In home care provider

The income of a live-in aid* or amounts paid by a State agency (In Home Supportive Services) to a family or non family member to offset the cost of services and equipment needed to keep the family member at home will not be included in total household income.

*Live-in aid means a person who resides with one or more elderly persons (at least 62 years old), or near elderly persons (at least 50 years old), or persons with disabilities, and who:

1. Is determined to be essential to the care and well-being of the person(s);
 2. Is not obligated for the support of the person(s); and
 3. Would not be living in the unit except to provide the necessary supportive services.
-

Income from a minor

Income from employment of children (including foster children) under the age of 18 years will be excluded from countable household income.

Disaster assistance

Payments made by federal service providers under a presidential declaration of disaster including, but not limited to, individual family grants from the Federal Emergency Management Agency (FEMA).

Victims of crime payments

All reparation payments to victims of a crime.

Reparation payments

Payments to Aleut people and people of Japanese ancestry under Public Law 100-383.

Victims of Nazi persecution

Payments made to individuals because of their status as victims of Nazi persecution shall be disregarded in determining eligibility.

Older volunteers

Older Americans Volunteers Act of 1965 – Income paid to participants in programs carried out under the Community Service Employment Program (Title V of the Older Americans Act), including Green Thumb, Senior Health Aides, Senior Companions.

Continued on next page

Excluded Income Sources, Continued

Older volunteers Older Americans Volunteers Act of 1965 – Income paid to participants in programs carried out under the Community Service Employment Program (Title V of the Older Americans Act), including Green Thumb, Senior Health Aides, Senior Companions.

Domestic volunteers Domestic Volunteer Service Act of 1973(P.L.93113) - Income paid to participants - Title I: Volunteers in Service to America (VISTA), Americorps, University Year for Action (UYA), Urban Crime Prevention Program. Title II: Retired Senior Volunteer Program (RSVP), Foster Grandparent Program, Older American Community Service Program (Senior Health Aides, Senior Companions). Title III: Service Corps of Retired Executives (ACE)

Vietnam veterans Vietnam Agent Orange Benefits. Benefits **given** for the children of woman-Vietnam veterans who suffer from certain birth defects must not be considered as income in determining eligibility or benefits.

Native American land The value of land taken from and later added back to Indian reservations must not be considered income.

Native American judgments Indian per capita judgment payments made to any tribe or group whose trust relationship with the federal government has been terminated and for which legislation was in effect before October 12, 1973 authorized the disposition of its judgment funds.

Non-cash Any non-cash Federal or State Benefits.

WIA Title I of the Workforce Investment Act of 1998: Supportive services to participants including assistance that enables people to participate in the program, such as transportation, health care, child care, handicapped assistance, meals, temporary shelter, counseling, and other reasonable expenses or participation in the program.

Continued on next page

Excluded Income Sources, Continued

Nutrition programs

Benefits from Women, Infant, and Children (WIC) program, Agriculture Nutrition Act of 1949 Section 416: value of federally donated food acquired through price support operations for school lunch or other distribution to needy people. Child Nutrition Act: the value of assistance to children under this Act. National School lunch Act: the value of assistance to children under this Act. Meals for Older Americans, School breakfasts and lunches and milk programs.

Job related expenses

For non self-employed applicants that do not file income tax as self employed (a sales person or a truck driver/taxicab driver) and who pays business expenses and also receives a paycheck, deduct ~~these~~ business expenses from the household's total gross income.

Employer paid benefits

Most employers providing benefits make a contribution to the cost of the benefit, with any remaining cost to be paid by the employee through payroll deduction. The employer contribution is not income. The payroll deduction is income.

Gifts and inheritances

One time lump sum inheritances or gifts. Such as gifts occasioned by a death or gifts of domestic travel tickets.

Prizes and awards

A prize is generally something received in a contest, lottery or game of chance. An award is usually received as the result of a decision by a court, board of arbitration, or the like.

Food stamps

The value of the coupon allotment provided to any eligible household.

Medicare and medical

The value of medical expenses paid directly to a health care provider on behalf of the household.

Medicare deductions

The deduction for Medicare from Social Security benefits.

Continued on next page

Excluded Income Sources, Continued

**Sale or
exchange of
property**

Capital gains people received (or losses they incur) from the sale of property, including stocks, bonds, a house, or a car (unless the person was engaged in the business of selling such property, in which case count the net proceeds as income from self-employment)

**Other
exclusions**

- Military combat pay
 - Child Support Payment contributions
 - Draw down from Reverse Mortgage
 - Tax Refunds
 - Loans
 - Withdrawal from Savings
 - Food or housing received in lieu of wages.
 - The value of food and fuel produced and consumed on farms
 - One-time Insurance Payments
 - Compensation for Injury
-