

ATTACHMENT 1
SAMPLE PROGRAM INTEGRITY ASSESSMENT SUPPLEMENT TEMPLATE
 Low Income Home Energy Assistance Program (LIHEAP)

ABSTRACT:

HHS is requiring further detail from States on their FY2011 plans for preventing and detecting fraud, abuse, and improper payments. HHS is also requiring that States highlight and describe all elements of this FY2011 plan which represent improvements or changes to the State's FY2010 plan for preventing and detecting fraud, abuse and improper payment prevention.

State, Tribe or Territory (and grant official): <i>Washington</i>	Date/Fiscal Year: <i>FY 2010</i>		
RECENT AUDIT FINDINGS			
Describe any audit findings of material weaknesses and reportable conditions, questioned costs and other findings cited in FY2010 or the prior three years. In annual audits, State 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 FY2011.	If there is no plan in place, please explain why not.	Necessary outcomes from these systems and strategies

No reported Audit findings.

The timely and thorough resolution of weaknesses or reportable conditions as revealed by the audit.

COMPLIANCE MONITORING

<p>Describe the State's FY2010 strategies that will continue in FY2011 for monitoring compliance with State and Federal LIHEAP policies and procedures by the State and local administering agencies.</p>	<p>Please highlight any strategies for compliance monitoring from your plan which will be newly implemented as of FY2011.</p>	<p>If you don't have a firm compliance monitoring system in place for FY11, please describe how the State is verifying that LIHEAP policy and procedures are being followed.</p>	<p>Necessary outcomes from these systems and strategies</p>
<p>The state of Washington currently has a system in place for all EAP sub grantees. We do an annual risk assessment, annual desk audit, and programs are on a 3 year schedule for onsite monitoring unless they are deemed high risk.</p>			<p>A sound methodology, with a schedule for regular monitoring and a more effective monitoring tool to gather information.</p>

FRAUD REPORTING MECHANISMS

<p>For FY2010 activities continuing in FY2011, 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.</p>	<p>Please highlight any tools or mechanisms from your plan which will be newly implemented in FY2011, and the timeline for that implementation.</p>	<p>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.</p>	<p>Necessary outcomes of these strategies and systems</p>
<p>State LIHEAP staff is accessed by phone or email. Phone numbers of LIHEAP staff are listed on our website. All LIHEAP associates are encouraged to report any problems or concerns to Commerce staff via website.</p> <p>In Washington we also use the fair hearing process for suspected fraud on behalf of our LIHEAP clients.</p> <p>All cases of reported fraud and abuse are taken on a case by case basis. At the state level we get all the facts we can from clients who call. We provide technical assistance to subcontractors who suspect potential clients of falsifying information.</p> <p>In Washington we do not</p>			<p><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></p>

prosecute but we will make the client provide additional documentation and start the process over if they falsify information.

VERIFYING APPLICANT IDENTITIES

<p>Describe all FY2010 State policies continuing in FY2011 for how identities of applicants and household members are verified.</p>	<p>Please highlight any policy or strategy from your plan which will be newly implemented in FY2011.</p>	<p>If you don't have a system in place for verifying applicant's identities, please explain why and how the State is ensuring that only authentic and eligible applicants are receiving benefits.</p>	<p>Necessary outcomes from these systems and strategies</p>
<p>We verify applicant identities by using state ID's, SS cards, and/or birth certificates for children. In most cases this can be verified through the state Benefit Verification System, which has information supplied by our department of Social and Health Services.</p>			<p><i>Income and energy supplier data that allow program benefits to be provided to eligible individuals.</i></p>

SOCIAL SECURITY NUMBER REQUESTS

<p>Describe the State's FY2011 policy in regards to requiring Social Security Numbers from applicants and/or household members applying for LIHEAP benefits.</p>	<p>Please describe whether the State's policy for requiring or not requiring Social Security numbers is new as of FY2011, or remaining the same.</p>	<p>If the State is not requiring Social Security Numbers of LIHEAP applicants and/or household members, please explain what supplementary measures are being employed to prevent fraud.</p>	<p>Necessary outcomes from these systems and strategies</p>
<p>Social security number documentation.</p> <p>When documenting an applicant's social security number, the contractor must:</p> <p>File either:</p> <p>A copy of the social security card; or</p> <p>A copy of other documentation or correspondence that shows both the name and social security number; or</p> <p>Written notification of the applicant's number from the local Social Security Administration; or</p> <p>A notation that the social security number had been verified from the DSHS Benefit Verification System; or</p>	<p>This is the same policy that we have had since before 2010.</p> <p>Currently there is no statewide system available specifically for the SS information. The department of Commerce will be entering into negotiations with other state agencies to determine accessibility of SS verification systems.</p>		<p><i>All valid household members are reported for correct benefit determination.</i></p>

CROSS-CHECKING SOCIAL SECURITY NUMBERS AGAINST GOVERNMENT SYSTEMS/DATABASES

<p>Describe if and how the State used existing government systems and databases to verify applicant or household member identities in FY2010 and continuing in FY2011. (Social Security Administration Enumeration Verification System, prisoner databases, Government death records, etc.)</p>	<p>Please highlight which, if any, policies or strategies for using existing government databases will be newly implemented in FY2011.</p>	<p>If the State won't be cross checking Social Security Numbers and ID information with existing government databases, please describe how the State will supplement this fraud prevention strategy.</p>	<p>Necessary outcomes from these systems and strategies</p>
<p>In WA we have access to a system that tracks income information as well as tracks clients with SSN's. This is through the Department of Social and Health services. Cross checking is limited to those clients that currently receive services such as TANF/SNAP.</p>		<p>In Washington there is currently no global data base that we can cross check against.</p> <p>WA does currently require SSN documentation. For those clients that are TANF/SNAP recipients we will cross check with Department of Social and Health Services Benefit Verification System.</p>	<p>Use of all available database systems to make sound eligibility determination.</p>
<p>VERIFYING APPLICANT INCOME</p>			
<p>Describe how the State or designee used State Directories of new hires or similar systems to confirm income eligibility in FY2010 and continuing in FY2011.</p>	<p>Please highlight any policies or strategies for using new hire directories which will be newly implemented in FY2011.</p>	<p>If the State won't be using new hire directories to verify applicant and household member incomes how will the State be verifying the that information?</p>	<p>Necessary outcomes from these systems and strategies</p>

		<p>An applicant must provide the names, gross income, and the source of income for all members of a shared household on the date of application.</p> <p>Contractors must use the Household Income Information Form, provided by the state, or a similar approved form.</p> <p>To verify earned income, contractors have the option to use pay stubs, an Employer Earned Income Form, or a similar approved form.</p> <p>For unearned income contractors rely on Social Security and DSHS documentation.</p>	<p><i>Effective income determination achieved through coordination across program lines.</i></p>
--	--	--	--

PRIVACY-PROTECTION AND CONFIDENTIALITY

<p>Describe the financial and operating controls in place in FY2010 that will continue in FY2011 to protect client information against improper use or disclosure.</p>	<p>Please highlight any controls or strategies from your plan which will be newly implemented as of FY2011.</p>	<p>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.</p>	<p>Necessary outcomes from these systems and strategies</p>
--	---	--	---

<p>W/A has a web based system for submission of LIHEAP client data. In addition to this we require that records be physically secured by subcontractors.</p> <p>Internet Explorer 5.01, 5.50, 6.0 or 7.0 installed and used as the World Wide Web browser. All versions must have the most recent IE Cumulative Update installed</p> <p>(http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp). This provides 128-bit client-side encryption of browser sessions. As future Service Packs, patches, or hotfixes are released by Microsoft, contractors will download and install them as directed by COMMERCE. A recommended 'Best Practice' would be to use the Windows Update feature to scan systems. Please work with your system administrator to coordinate patch management</p> <p>(http://v4.windowsupdate.microsoft.com/en/default.asp).</p> <p>'Strong' password authentication - passwords must include at least one lower-case alphabetic character (a to z), at least one upper-case character (A to Z), and at least one non-alphabetic character (*,\$,#,1-9, etc.,). Passwords are also required to be at least 8 characters long, are case sensitive, and must be changed every 60 days. You cannot use common words, names, religious or sports references.</p> <p>EAP Coordinators will manage user-id and passwords for staff. This includes notifying COMMERCE immediately when staff end employment or are reassigned, and deleting their user-id and password. Each user is allowed one user-id and password at any time.</p>		<p>why.</p>	<p>Clear and secure methods that maintain confidentiality and safeguard the private information of applicants.</p>
--	--	-------------	--

Any contractor wishing to use wireless Internet connections ('Wi-Fi') must contact COMMERCE prior to using a Wi-Fi equipped device in conjunction with client service. Wireless connections are inherently insecure unless the following minimum steps are taken:

- Block the SSID (Service Set ID) from transmitting.
- Use a personal firewall, antivirus, and anti-spyware software.
- Use WPA (Wireless Protected Access) and change WPA keys frequently.
- Use VPN (Virtual Private Network) software to connect to your office network.

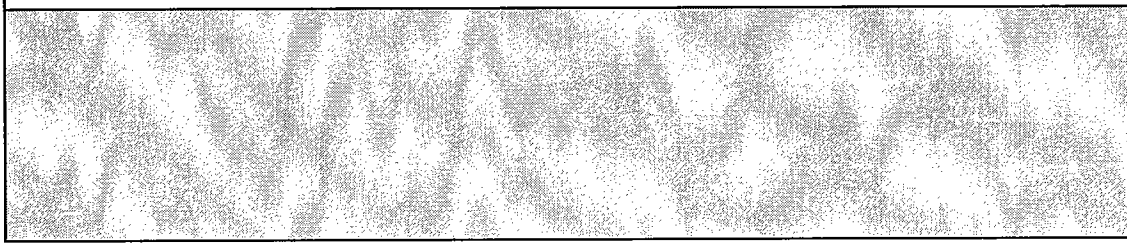
Contractors will shred any unnecessary paper documents containing client information daily.

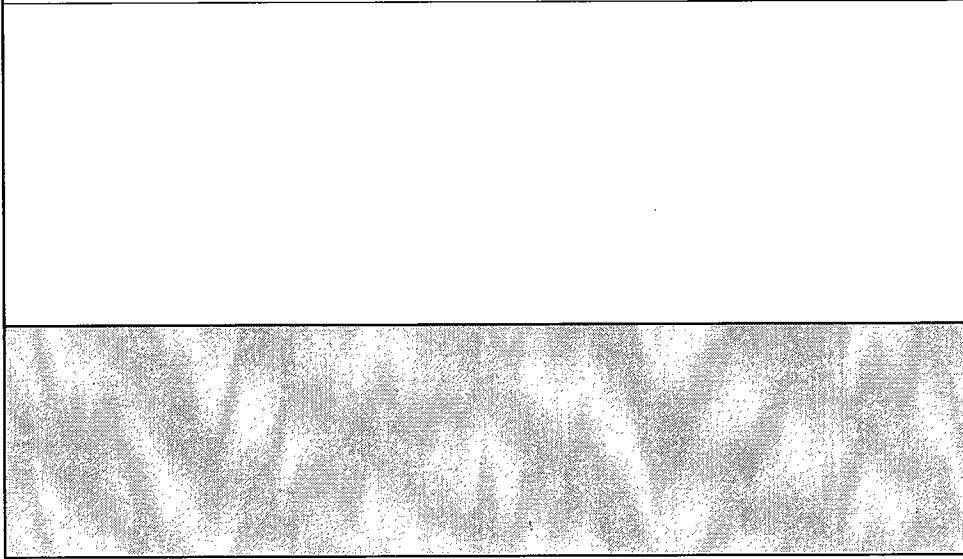
Access to the secure website will be limited to authorized users during regular working hours daily, and restricted at night and on the weekends, unless by prior authorization. COMMERCE will use IP address monitoring to track individual usage. Contractors may use home systems to connect to the secure site only if they have personal firewalls and anti-virus software in use and updated regularly.

Each authorized user will review Policy 4.6.4, sign and return the Contractor Statement of Assurance form, which acknowledges compliance with the above policies and commitment to information security, client privacy and confidentiality.

As per our contract:
CLIENT PRIVACY STANDARDS

Personal information collected by Commerce, used or acquired in connection with any state-funded program shall be used solely for the



<p>purpose of that program. Contractors agree not to release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons the personal information without express written consent of the client or as provided by law. The written consent must include what client information may be shared and to whom or which agencies/businesses. Contractors agree to implement physical, electronic and managerial safeguards to prevent unauthorized access to personal information.</p> <p>Personal information includes but is not limited to information that would identify an individual's health, education, business, use or receipt of governmental services, names, addresses, age, telephone numbers, social security numbers, driver license numbers and finances including financial profiles, credit card numbers or other identifying numbers.</p> <p>COMMERCE reserves the right to monitor, audit or investigate the use of personal information collected by Commerce, used or acquired by the Contractors. Not properly maintaining clients' private information could result in termination of the contract or subcontract. Contractors agree to indemnify and hold harmless COMMERCE, the State and its officers, employees and authorized agents for any damages related to the Contractor's unauthorized use of personal information.</p> <p>Contractors shall include this client privacy policy in all subcontracts. In addition, Contractors shall include in the subcontract a clause stating that Subcontractors agree to indemnify and hold harmless the Contractor, the State and its officers, employees and authorized agents for any damages related to the Subcontractor's unauthorized use of personal information. Contractors have the responsibility to monitor the use of personal information collected by Commerce by Subcontractors.</p>		
--	--	--

LIHEAP BENEFITS POLICY

<p>Describe FY2010 State policies continuing in FY2011 for protecting against fraud when making payments, or providing benefits to energy vendors on behalf of clients.</p>	<p>Please highlight any fraud prevention efforts relating to making payments or providing benefits which will be newly implemented in FY2011.</p>	<p>If the State 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 State taking to ensure program integrity.</p>	<p>Necessary outcomes from these systems and strategies</p>
<p>Policy 4.5.1 (B): EAP Benefits Provided By Two Methods</p> <p>EAP benefits will be made to an eligible household as a payment to the household's heating energy vendor (oil company, electric utility, gas company, etc.), on behalf of the household, or through direct payment to the applicant. In 2009 94% of LIHEAP benefits were paid directly to the client's account at their Utility/Energy Vendor.</p> <p>LIHEAP system flags double payments through last name and/or SSN. Contractors require income information and can check through the BVS system if client is DSHS client.</p> <p>Policy 4.5.1 (C): Payment To Vendors Requires Signed</p>			<p>Authorized energy vendors are receiving payments on behalf of LIHEAP eligible clients.</p>

