



CDSS

JOHN A. WAGNER
DIRECTOR

STATE OF CALIFORNIA—HEALTH AND HUMAN SERVICES AGENCY
DEPARTMENT OF SOCIAL SERVICES



ARNOLD SCHWARZENEGGER
GOVERNOR

August 26, 2008

ALL-COUNTY INFORMATION NOTICE NO I-62-08

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY SPECIAL INVESTIGATIVE UNIT CHIEFS
ALL COUNTY INCOME AND ELIGIBILITY
VERIFICATION SYSTEM COORDINATORS
WELFARE INTERCEPT COORDINATORS

SUBJECT: CONFIDENTIAL TAX INFORMATION SAFEGUARD REQUIREMENTS

REFERENCE: 26 USC § 6103; INTERNAL REVENUE PUBLICATION 1075, TAX
INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND
LOCAL AGENCIES

<u>REASON FOR THIS TRANSMITTAL</u>
<input type="checkbox"/> State Law Change
<input type="checkbox"/> Federal Law or Regulation Change
<input type="checkbox"/> Court Order
<input type="checkbox"/> Clarification Requested by One or More Counties
<input checked="" type="checkbox"/> Initiated by CDSS

The purpose of this All County Information Notice (ACIN) is to ensure county compliance with state and federal confidential data security requirements.

Federal law requires agencies using confidential state and federal tax information (FTI) to prevent unauthorized release of confidential information (26 USC § 6103). IRS Publication 1075, "Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities," provides guidance on how to prevent unauthorized release of FTI. Failure to adhere to IRS security guidelines can lead to termination of access to FTI.

County collections staff receive FTI as processed by the Welfare Intercept System (WIS). Collections staff use WIS to intercept tax return money in order to recover Food Stamp Program over issuances. Counties receive incentive payments from intercepted funds.

County Income Eligibility Verification System (IEVS) workers use FTI to identify income and assets which aid recipients may not have reported in order to qualify for aid, or to qualify for a larger grant while on aid. IEVS workers identify overpayments for collection by using FTI – based IEVS matches, including the FTB and IRS Asset matches. Losing access to FTI may prevent IEVS workers from identifying all overpayments that could be recovered by collection or tax intercept actions.

Federal law and regulations, explained in IRS Publication 1075, require state and county agencies to perform specific actions to ensure continuing access to confidential tax information:

- Agencies are required to reduce the risk of unauthorized release of FTI in communications with public and private parties. (26 USC § 6103 (p)(4).) A Verification of Employment/Earnings letter formatted to reduce the risk of confidential information disclosure (attachment 1) has been supplied by IRS. Use the letter as the template for third party verification letters sent out by county agencies to employers or other parties to verify IEVS match results.
- Annually complete the County Internal Inspection and Safeguard Activity Report (attachment 2). (26 USC § 6103 (p)(4).) Counties must perform the internal inspection, fill out the report, and send the report in to the California Department of Social Services (CDSS) Fraud Bureau by September 15th.
- The IRS also requires State and county agencies to complete a Safeguard Procedure Report (attachment 3). (26 USC § 6103 (p)(4).) The report should be completed and turned in to CDSS Fraud Bureau by March 1, 2009.
- The IRS further requires agencies to provide safeguard training to all employees who handle FTI, per Publication 1075. In addition to training, employees who handle FTI should be provided with a copy of Exhibits 5 and 7 from Publication 1075 (attachment 4). These exhibits explain the civil and criminal penalties for unauthorized access or disclosure of FTI.
- Annual verification of training for all employees who handle FTI must arrive at the CDSS Fraud Bureau by September 15th. The county IEVS coordinator confirms that the training has been completed, then fills out and signs a County Certification Letter (attachment 5) which is forwarded to the Fraud Bureau's IRS Coordinator.
- Any contractor or sub-contractor (janitor, private security guard) who might encounter FTI must be informed of the civil and criminal penalties of unauthorized access or disclosure of FTI. (26 USC § 6103 (d).) Provide a copy of Exhibit 7 (attachment 6) to any contracted worker who might encounter FTI.
- Contractors and sub-contractors need to sign the Sub-Contractor Certification Letter (attachment 7). The county IEVS coordinator should send any original signed sub-contractor letters to CDSS Fraud Bureau no later than September 15th of each year.

All original signed internal inspection reports and original signed certification letters due to CDSS Fraud Bureau by September 15th of each year should be sent to:

CDSS Fraud Bureau
744 P Street, MS 19-26
Sacramento, CA 95814
ATTN: IRS Coordinator

All County Information Notice No. I-62-08
Page Three

If you have questions concerning this letter or attachments, please contact June Ramos of the CDSS Fraud Bureau at (916) 263-5700.

Sincerely,

Original Document Signed By:

GARY GRAYSON, Chief
Welfare Fraud and Emergency Food Assistance Program Bureau

Attachments

County of

DEPARTMENT OF

District Stamp

Date:
Case Name:
Case Number:
File No.:
Worker Name:
Telephone:

VERIFICATION OF EMPLOYMENT / EARNINGS

Dear Employer:

Re: _____ SSN: _____

Your tax dollars help fund public assistance programs for needy persons. Your cooperation is needed to ensure that only eligible persons receive public assistance and in the correct amount.

The above named participant has been identified by the Employment Development Department (EDD) as an employee of your firm. According to our records, this information differs from what the participant has reported to us.

To resolve this discrepancy, please complete, sign, date and return page two in the enclosed postage paid envelope within **ten (10)** days from the date of this letter. If the participant **is not** or **was never** employed by your firm, please check the box located on the bottom of page two, sign and correct your records to prevent further inquiries of this nature. Please provide all the information on the attached form and **destroy this cover letter**.

Also, for your information, unresolved information related to employment and earnings may be referred to the District Attorney's Office as required by State law.

Information contained in this letter and obtained on the attached form is confidential under federal regulations, IRC Sec. 6103 of the Internal Revenue Code. This information will not be released except as permitted or required by law or with the written consent of the participant.

Thank you for your cooperation.

Sincerely,

IEVS/IFDS Eligibility Worker

() _____
Telephone Number

Enclosures

**Annual County Internal Inspection
and Safeguard Activity Report**

This report must be completed annually by each county. Send the original to:

CDSS Fraud Bureau
744 P Street, MS 19-26
ATTN: IRS Coordinator
Sacramento, CA 95814

- Save a copy in the file the county uses for IRS Safeguard activity.
- Part A – Welfare Intercept System (WIS): WIS is the State – moderated program which connects county collections with the federal Tax Offset program (TOP). Accessing federal tax return and benefit data through TOP requires adherence to federal data security guidelines.
- Part B – IEVS: Several IEVS matches utilize federal wage and benefit information. Accessing federal wage and benefit information requires adherence to federal data security guidelines.
- Resources:
 - IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities.
 - IRS Publication 3373 (5-2007) Disclosure of Information to Federal, State, and Local Agencies.
 - NIST FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems.

County

Date

PART A – WIS

1.	Who receives IRS data from CDSS Fraud Bureau? Include name and contact phone number.
2.	How is receipt of the data documented and maintained?

3.	Where are the documents stored?
4.	How is IRS information access granted to employees?
5.	Do employees receive annual IRS security training and is signed certification by the employee on file regarding the penalties associated with unauthorized disclosure?
6.	Does the county conduct an awareness program to ensure employees remain alert to all security requirements and penalties for unauthorized disclosure of IRS data (bulletin boards, newsletters, posters, videos)?
7.	Has there been any change to the person(s) authorized to access federal tax information (FTI)? If yes, who is the new person(s) authorized?
8.	Does the county have security procedures and instruction for employees?
9.a.	What are the facility's security procedures?
9.b.	Describe the county's external building security.
9.c.	Describe the county's internal area security where the IRS data is used (type of lock, alarm, safe, container).

9.d.	Describe the county's after hours security.
10.	Who has access to the safe or other secure storage container in which IRS data is stored?
11.	Who is responsible for changing keys or safe combinations?
12.	What measures are taken to ensure that IRS data is not co-mingled with the continuing eligibility case records, both in case files and in computer data systems?
13.	What are the county procedures for disposing of IRS data (Shredding? Burning? If contracted out, is the data medium shredded prior to pickup? If contracted out, provide a copy of the contract.)? No shredding by a contractor is to take place unless observed and documented by an authorized "welfare" agency staff person. A 5/16" criss-cross shredder is applicable for in-house shredding. Provide a copy of the disposal log.
14.	What activities occur in the area where IRS data is secured?
15.	Describe the county's computer security for system equipment, data receipt and storage, and accessibility with regard to the handling and storage of FTI.
16.	Has any FTI been disclosed to any State, County, or other external auditor? If yes, explain:

17.	Have there been any changes since submission of the county's last Annual Internal Inspection/Safeguard Activity Report? If so, what are they?
18.	If deficiencies are noted in the above areas, what corrective action will be taken by the county to ensure that all IRS safeguard procedures are met?
19.	Name(s) and title(s) of county personnel completing this report:

Signature of Inspector

Date

PART B – IEVS

1.	Who receives IRS data from CDSS Fraud Bureau? Include name and contact phone number.
2.	How is receipt of the data documented and maintained?
3.	Where are the documents stored?
4.	How is IRS information access granted to employees?
5.	Do employees receive annual IRS security training and is signed certification by the employee on file regarding the penalties associated with unauthorized disclosure?

6.	Does the county conduct an awareness program to ensure employees remain alert to all security requirements and penalties for unauthorized disclosure of IRS data (bulletin boards, newsletters, posters, videos)?
7.	Has there been any change to the person(s) authorized to access federal tax information (FTI)? If yes, who is the new person(s) authorized?
8.	Does the county have security procedures and instruction for employees?
9.a.	What are the facility's security procedures?
9.b.	Describe the county's external building security.
9.c.	Describe the county's internal area security where the IRS data is used (type of lock, alarm, safe, container).
9.d.	Describe the county's after hours security.
10.	Who has access to the safe or other secure storage container in which IRS data is stored?
11.	Who is responsible for changing keys or safe combinations?

12.	What measures are taken to ensure that IRS data is not co-mingled with the continuing eligibility case records, both in case files and in computer data systems?
13.	What are the county procedures for disposing of IRS data (Shredding? Burning? If contracted out, is the data medium shredded prior to pickup? If contracted out, provide a copy of the contract.)? No shredding by a contractor is to take place unless observed and documented by an authorized "welfare" agency staff person. A 5/16" criss-cross shredder is applicable for in-house shredding. Provide a copy of the disposal log.
14.	What activities occur in the area where IRS data is secured?
15.	Describe the county's computer security for system equipment, data receipt and storage, and accessibility with regard to the handling and storage of FTI.
16.	Has any FTI been disclosed to any State, County, or other external auditor? If yes, explain:
17.	Have there been any changes since submission of the county's last Annual Internal Inspection/Safeguard Activity Report? If so, what are they?
18.	If deficiencies are noted in the above areas, what corrective action will be taken by the county to ensure that all IRS safeguard procedures are met?
19.	Name(s) and title(s) of county personnel completing this report:

Signature of Inspector

Date

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

**Dated:
Reviewed:**

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed
1. Responsible Officer(s)			
1.1	<i>Is the name, title, address, and telephone number of the agency official authorized to request Federal tax information from the IRS, the SSA, or other authorized agency documented?</i>	John A. Wagner, Director California Department of Social Services 744 P Street MS 17-11 Sacramento, CA 95814 (916) 657-2598	
1.2	<i>Is the name, title, address, and telephone number of the agency official responsible for implementing the safeguard procedures documented?</i>	Gary Grayson, Chief Welfare Fraud and Emergency Food Assistance Program Bureau 744 P Street MS 19-26 Sacramento, CA. 95814 (916) 263-5524	
2. Location of the Data			
2.1	<i>Is an organizational chart or narrative description of the receiving agency, which includes all functions within the agency where FTI will be processed or maintained, documented?</i> Note: <i>If the information is to be used or processed by more than one function, then the pertinent information must be included for each function.</i>	The California Department of Social Services (CDSS) organizational structure is enclosed as Enclosure A. Enclosure B is the organizational structure of the Fraud Bureau which has responsibility for providing and maintaining the safeguard procedures. The physical location of the data is 2525 Natomas Park Drive, Suite 250, Sacramento, California 95833.	
3. Flow of the Data			
3.1	<i>Is there a chart or narrative describing:</i> • <i>the flow of FTI through the agency from its</i>	Check with Jeff Adge. Also need:	

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	<p><i>receipt through its return to the IRS or its destruction,</i></p> <ul style="list-style-type: none"> <i>how it is used or processed, and</i> <i>how it is protected along the way</i> 	<ul style="list-style-type: none"> California Department of Social Services – Internal Revenue Service Special Procedures Report. Flow charts of processes. 	
3.2	<i>Is commingled or transcribed FTI data kept by the agency described and documented in the procedures?</i>	Check with Jeff Adge	
3.3	<i>Is any data turned over to an agency contractor for processing fully disclosed and provided accurate accounting?</i>	Check with Jeff Adge	
4. System of Records			
4.1	<p><i>Is a description of the permanent record(s) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes or cartridges or other Page 34 removable media) specified?</i></p> <p>Note: Agencies are expected to be able to provide an "audit trail" for information requested and received, including any copies or distribution beyond the original document or media.</p>		
5. Secure Storage of the Data			
5.1	<p><i>Is a description of the security measures employed to provide secure storage for the data when it is not in current use documented?</i></p> <p><i>Note: Secure storage encompasses such considerations as locked files or containers, secured facilities, key or combination controls, offsite storage, and restricted areas.</i></p> <p>For Federal Agencies, it is requested that they submit a Vulnerability Assessment based on General Services Administration standards for their building(s) as it addresses physical security.</p>		
6. Restricting Access to the Data			
6.1	<p><i>Is there a documented description of the procedures or safeguards to ensure access to FTI is limited to those individuals who are authorized access and have a need to know? This includes a description of:</i></p> <ul style="list-style-type: none"> <i>How the information will be protected from unauthorized access when in use by the authorized recipient,</i> 		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	<ul style="list-style-type: none"> • <i>The physical barriers to unauthorized access (including the security features where FTI is used or processed), and</i> • <i>Systemic or procedural barriers.</i> 		
<i>7. Disposal</i>			
<p>7.1</p>	<p><i>Is a description of the method(s) of FTI disposal (when not returned to the IRS) documented?</i></p> <p>Note: <i>The IRS will request a written report that documents the method of destruction and that the records were destroyed.</i></p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

8. Computer Security

8.1 *Name and Address of Data Center:*

Name, telephone number, and e-mail address of Security Administrator or other IT contact at the Data Center:

Is this facility shared by other State agencies?

A brief description of FTI data flow within all automated information systems and networks that receive, process, store, or transmit FTI:

Brief description of IT environment:

1-Mainframe: e.g. IBM/Unisys

Operating System: e.g. zOS v1.7

Security Software: RACF

No. of production LPARs with FTI:

2-UNIX/LINUX:

Operating System: e.g. Solaris v2.8

No. of production Servers with FTI: e.g. 4

Operating System: e.g. Red Hat v5.6

No. of production Servers with FTI: e.g. 2

3-Windows:

Operating System: e.g. Windows 2003

No. of production Servers with FTI: e.g. 4

Operating System: e.g. Windows 2002

No. of production Servers with FTI: e.g. 1

4-Tumbleweed:

Operating System: e.g. Windows 2003

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	(server/workstation)		
	No. of production Servers with FTI: e.g. 1		
8.2	MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: RISK ASSESSMENT		
	<i>RA1</i> PUBLICATION 1075 GUIDANCE: Risk assessment policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing risk assessment controls. Such risk assessment controls include risk assessments and risk assessment updates.		
	<i>RA3</i> PUBLICATION 1075 GUIDANCE: Agencies must conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of FTI		
	<i>RA4</i> PUBLICATION 1075 GUIDANCE: The agency must update the risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system		
	<i>RA5</i> PUBLICATION 1075 GUIDANCE: Periodically, systems that contain FTI shall be scanned to identify vulnerabilities in the information system. The agency shall identify the timeframe on how often scans are conducted.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

8.3	MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: SECURITY PLANNING		
PL1	PUBLICATION 1075 GUIDANCE: Security planning policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing security planning controls. Such security planning controls include system security plans, system security plan updates and rules of behavior.		
PL2	PUBLICATION 1075 GUIDANCE: Agencies must develop, document, and establish a system security plan by describing the security requirements, current controls and planned controls, for protecting agency information systems and Federal tax information.		
PL3	PUBLICATION 1075 GUIDANCE: The system security plan must be updated to account for significant changes in the security requirements, current controls and planned controls for protecting agency information systems and Federal tax information.		
PL4	PUBLICATION 1075 GUIDANCE: Agencies must develop, document, and establish a set of rules describing their responsibilities and expected behavior for information system use for users of the information system.		
PL6	PUBLICATION 1075 GUIDANCE: The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

8.4	MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND SERVICES ACQUISITION			
	SA1	PUBLICATION 1075 GUIDANCE: System and services acquisition policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing system and services acquisition controls. Such system and services acquisition controls include information system documentation and outsourced information system services. Agencies must ensure that there is sufficient information system documentation, such as a Security Features Guide. Agencies must ensure third-party providers of information systems, who are used to process, store and transmit Federal tax information, employ security controls consistent with Safeguard computer security requirements.		
	SA2	PUBLICATION 1075 GUIDANCE: The agency shall document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.		
	SA3	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency manages the information system using a system development life cycle methodology that includes information security considerations.		
	SA4	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.		
	SA5	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency shall obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.		
	SA6	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency complies with software usage restrictions.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	SA7	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency shall enforce explicit rules governing the installation of software by users.		
	SA8	PUBLICATION 1075 GUIDANCE: Whenever information systems contain FTI, the agency shall design and implement the information system using security engineering principles.		
	SA11	PUBLICATION 1075 GUIDANCE: The information system developers shall create a security test and evaluation plan, implement the plan, and document the results.		
8.5	MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: CERTIFICATION & ACCREDITATION (C&A)			
	CA1	PUBLICATION 1075 GUIDANCE: The agency shall develop and update a policy that addresses the processes used to test, validate, and authorize the security controls used to protect FTI. While state and local agencies are not required to conduct a NIST compliant C&A, the agency shall accredit in writing that the security controls have been adequately implemented to protect FTI. The written accreditation constitutes the agency's acceptance of the security controls and associated risks. However for federal agencies that receive FTI, a NIST compliance C&A is required in accordance with FISMA.		
	CA2	PUBLICATION 1075 GUIDANCE: The agency shall conduct an assessment of the security controls in the information system, periodically but at least annually, to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This assessment shall complement the certification process to ensure that periodically the controls are validated as being operational.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

CA3	<p>PUBLICATION 1075 GUIDANCE: The agency shall authorize and document all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.</p>		
CA4	<p>PUBLICATION 1075 GUIDANCE: The agency shall conduct a formal assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.</p>		
CA 5	<p>PUBLICATION 1075 GUIDANCE: As recipients of FTI, the agency is responsible to develop and update a Plan of Action and Milestones (POA&M) that shall identify any deficiencies related to FTI processing. The POA&M shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during the review processes, either internal or external. The POAM shall address implementation of security controls to reduce or eliminate known vulnerabilities in the system.</p>		
CA 6	<p>PUBLICATION 1075 GUIDANCE: Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security accreditation. All information regarding the accreditation shall be provided to the Office of Safeguards as part of the Safeguard Activity Report.</p>		
CA7	<p>PUBLICATION 1075 GUIDANCE: All agencies shall periodically, at least annually, monitor the security controls within the information system hosting FTI to ensure that the controls are operating, as intended.</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

8.6	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: PERSONNEL SECURITY		
	<p><i>PS1</i> PUBLICATION 1075 GUIDANCE: Personnel security policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing personnel security controls. Such personnel security controls include position categorization, personnel screening, personnel termination, personnel transfer, and access agreements.</p>		
	<p><i>PS2</i> PUBLICATION 1075 GUIDANCE: Agencies must assign risk designations to all positions and establish screening criteria for individuals filling those positions.</p>		
	<p><i>PS3</i> PUBLICATION 1075 GUIDANCE: Individuals must be screened before authorizing access to information systems and information.</p>		
	<p><i>PS4</i> PUBLICATION 1075 GUIDANCE: Agencies must terminate information system access, conduct exit interviews, and ensure return of all information system-related property when employment is terminated.</p>		
	<p><i>PS5</i> PUBLICATION 1075 GUIDANCE: Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.</p>		
	<p><i>PS6</i> PUBLICATION 1075 GUIDANCE: Appropriate access agreements must be completed before authorizing access to users requiring access to the information system and Federal Tax Information.</p>		
	<p><i>PS7</i> PUBLICATION 1075 GUIDANCE: Personnel security requirements must be established for third-party providers and monitored for provider compliance.</p>		
	<p><i>PS8</i> PUBLICATION 1075 GUIDANCE: Agencies must also establish a formal sanctions process for personnel who fail to comply with established information security policies, as this relates to FTI.</p>		
8.7	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: CONTINGENCY PLANNING		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

<p>CP1 CP2</p>	<p>PUBLICATION 1075 GUIDANCE: All FTI information that is transmitted to the states is backed up and protected within IRS facilities. As such, the controls of IT Contingency Planning are not required at the federal, state, or local agency. The primary contingency shall be to contact the IRS to obtain updated FTI data. If this timeframe extends beyond the IRS normal 60 day recovery period, agencies may not have immediate recovery of this information. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches. If FTI is included in contingency planning; policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing contingency planning security controls.</p>		
<p>CP4</p>	<p>PUBLICATION 1075 GUIDANCE: Plans must be periodically tested to ensure procedures and staff personnel are able to provide recovery capabilities within established timeframes. Such contingency planning security controls include alternate storage sites, alternate processing sites, telecommunications services, and information system and information backups.</p>		
<p>CP6</p>	<p>PUBLICATION 1075 GUIDANCE: Agencies must identify alternate storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups.</p>		
<p>CP7</p>	<p>PUBLICATION 1075 GUIDANCE: Agencies must identify alternate processing sites and/or telecommunications capabilities, and initiate necessary agreements to facilitate secure resumption of information systems used to process, store and transmit FTI if the primary processing site and/or primary telecommunications capabilities become unavailable.</p>		
<p>8.8</p>	<p>OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: CONFIGURATION MANAGEMENT</p>		
<p>CM1</p>	<p>PUBLICATION 1075 GUIDANCE:</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	Configuration management policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing configuration management security controls.		
CM2	PUBLICATION 1075 GUIDANCE: The organization develops, documents, and maintains a current baseline configuration of the information system.		
CM3	PUBLICATION 1075 GUIDANCE: Authorize, document, and control changes to the information system.		
CM4	PUBLICATION 1075 GUIDANCE: Monitor changes to the information system conducting security impact analysis to determine the effects of the changes.		
CM5	PUBLICATION 1075 GUIDANCE: Approve individual access privileges and enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes.		
CM6	PUBLICATION 1075 GUIDANCE: The agency shall establish mandatory configuration settings for information technology products employed within the information system, which (i) configures the security settings of information technology products to the most restrictive mode consistent with operational requirement; (ii) documents the configuration settings; and (iii) enforces the configuration settings in all components of the information system.		
CM7	PUBLICATION 1075 GUIDANCE: Restrict access for change, configuration settings, and provide the least functionality necessary. Enforce access restrictions associated with changes to the information system. Configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements. Configure the information system to provide only essential capabilities. Prohibit the use of functions, ports, protocols, and services not required to perform essential capabilities for		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		processing, storing, or transmitting Federal tax information.		
	CM8	PUBLICATION 1075 GUIDANCE: Develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.		
8.9	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: MAINTENANCE			
	MA1	PUBLICATION 1075 GUIDANCE: Maintenance policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing maintenance security controls. Such maintenance security controls include identifying and monitoring a list of maintenance tools and remote maintenance tools.		
	MA2	PUBLICATION 1075 GUIDANCE: The agency must ensure that maintenance is scheduled, performed, and documented. The agency must review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.		
	MA3 MA4	PUBLICATION 1075 GUIDANCE: Agencies must approve, control, and routinely monitor the use of information system maintenance tools and remotely-executed maintenance and diagnostic activities.		
	MA5	PUBLICATION 1075 GUIDANCE: The agency allows only authorized personnel to perform maintenance on the information system.		
8.10	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND INFORMATION INTEGRITY			
	SI1	PUBLICATION 1075 GUIDANCE: System and information integrity policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing system and information integrity security controls. Such system and information integrity security controls include flaw remediation,		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		intrusion detection tools and techniques, information input restrictions, and information output handling and retention.		
	SI2	PUBLICATION 1075 GUIDANCE: Agencies must identify, report, and correct information system flaws.		
	SI3	PUBLICATION 1075 GUIDANCE: The information system must implement protection against malicious code (e.g., viruses, worms, Trojan horses) that, to the extent possible, includes a capability for automatic updates.		
	SI4	PUBLICATION 1075 GUIDANCE: Intrusion detection tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of the information system and FTI.		
	SI5	PUBLICATION 1075 GUIDANCE: The agency shall receive and review information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.		
	SI9	PUBLICATION 1075 GUIDANCE: Agencies must restrict information system input to authorized personnel (or processes acting on behalf of such personnel) responsible for processing, storing, or transmitting FTI.		
	SI12	PUBLICATION 1075 GUIDANCE: Agencies must handle and retain output from the information system, as necessary to document that specific actions have been taken.		
8.11	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: INCIDENT RESPONSE			
	IR1	PUBLICATION 1075 GUIDANCE: Incident response policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate the implementing incident response security controls. Such incident response security controls include incident response training and incident reporting and monitoring.		
	IR2	PUBLICATION 1075 GUIDANCE: Agencies must train personnel in their		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		incident response roles on the information system and FTI. Incident response training must provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication, and recovery.		
	IR3	PUBLICATION 1075 GUIDANCE: The agency shall test and/or exercise the incident response capability for the information system at least annually to determine the incident response effectiveness and documents the results.		
	IR5	PUBLICATION 1075 GUIDANCE: Agencies must routinely track and document information system security incidents potentially affecting the confidentiality of FTI.		
	IR6	PUBLICATION 1075 GUIDANCE: Any time there is a compromise to FTI, the agency promptly reports incident information to the appropriate Agent-in-Charge, TIGTA.		
	IR7	PUBLICATION 1075 GUIDANCE: The agency shall also provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability.		
8.12	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: SECURITY AWARENESS AND TRAINING			
	AT1	PUBLICATION 1075 GUIDANCE: Awareness and training policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing awareness and training security controls. Such awareness and training security controls include security awareness and security training.		
	AT2	PUBLICATION 1075 GUIDANCE: Agencies must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to the system.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	AT3	PUBLICATION 1075 GUIDANCE: Agencies must identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities and provide sufficient security training before authorizing access to the information system and FTI.		
	AT4	PUBLICATION 1075 GUIDANCE: Agencies must document and monitor individual information system security training activities including basic security awareness training and specific information system security training.		
8.13	OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: MEDIA ACCESS PROTECTION			
	MP1	PUBLICATION 1075 GUIDANCE: Media access policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing media protection policy. Policies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls.		
	MP2	PUBLICATION 1075 GUIDANCE: The agency shall restrict access to information system media to authorized individuals, where this media contains FTI.		
	MP4	PUBLICATION 1075 GUIDANCE: The agency will physically control and securely store information system media within controlled areas, where this media contains FTI.		
	MP5	PUBLICATION 1075 GUIDANCE: All media being transmitted from the IRS must employ the use of encryption.		
	MP6	PUBLICATION 1075 GUIDANCE: The agency shall sanitize information system media prior to disposal or release for reuse.		
8.14	TECHNICAL SECURITY CONTROLS CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION			
	IA1	PUBLICATION 1075 GUIDANCE: Identification and authentication policy and procedures must be developed, documented, disseminated, and updated, as necessary, to facilitate implementing		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		identification and authentication security controls.		
	IA2 IA3	PUBLICATION 1075 GUIDANCE: The information system must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics.		
	IA4	PUBLICATION 1075 GUIDANCE: Agencies also must manage the user accounts assigned to the information system. Examples of effective user-account management practices include (i) obtaining authorization from appropriate officials to issue user accounts to intended individuals; (ii) disabling user accounts timely; (iii) archiving inactive or terminated user accounts; and (iv) developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by the information system.		
	IA6	PUBLICATION 1075 GUIDANCE: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
	IA7	PUBLICATION 1075 GUIDANCE: Whenever agencies are employing cryptographic modules, the agency shall work to ensure these modules are compliant with NIST guidance, including FIPS 140-2 compliance.		
8.15	TECHNICAL SECURITY CONTROLS CONTROL FAMILY: ACCESS CONTROL			
	AC1	PUBLICATION 1075 GUIDANCE: Access control policy and procedures must be developed, documented, disseminated, and updated, as necessary, to facilitate implementing access control security controls. Security controls include account management, access enforcement, limiting access to those with a need-to-know, information-flow enforcement, separation of		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		duties, least privilege, unsuccessful login attempts, system use notification, session locks, session termination, and remote access.		
AC2		PUBLICATION 1075 GUIDANCE: Agencies must manage information system user accounts, including establishing, activating, changing, reviewing, disabling, and removing user accounts.		
AC3 AC4		PUBLICATION 1075 GUIDANCE: The information system must enforce assigned authorizations for controlling system access and the flow of information within the system and between interconnected systems.		
AC5		PUBLICATION 1075 GUIDANCE: Agencies must ensure the information system enforces separation of duties through assigned access authorizations.		
AC6		PUBLICATION 1075 GUIDANCE: The information system must enforce the most restrictive access capabilities users need (or processes acting on behalf of users) to perform specified tasks.		
AC7		PUBLICATION 1075 GUIDANCE: The information system must limit the number of consecutive unsuccessful access attempts allowed in a specified period and automatically perform a specific function (e.g., account lockout, delayed logon) when the maximum number of attempts is exceeded.		
AC8		PUBLICATION 1075 GUIDANCE: The information system must display an approved system usage notification before granting system access informing potential users that (i) the system contains U.S. Government information; (ii) users actions are monitored and audited; and (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties. Policy must be enforced so that a workstation and/or application are locked after a pre-defined period. This will ensure that unauthorized staff or staff without a need-to-know cannot access FTI.		
AC12		PUBLICATION 1075 GUIDANCE: The information system shall automatically		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	terminate any remote session after fifteen minutes of inactivity, where these systems contain FTI. For instances of interactive and/or batch processing, compensating controls must be implemented.		
AC13	PUBLICATION 1075 GUIDANCE: Management must supervise and review the activities of the users as this relates to information system access.		
AC14	PUBLICATION 1075 GUIDANCE: In addition, the agency must identify and document specific user actions that can be performed on the information system without identification or authentication. Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible web site for which no authentication is required.		
AC17	PUBLICATION 1075 GUIDANCE: Agencies must authorize, document, and monitor all remote access capabilities used on the system, where these systems containing FTI.		
AC18	PUBLICATION 1075 GUIDANCE: Agencies must develop policies for any allowed wireless access, where these systems contain FTI. As part of the wireless access, the agency shall authorize, document, and monitor all wireless access to the information system.		
AC19	PUBLICATION 1075 GUIDANCE: Agencies must develop policies for any allowed portable and mobile devices, where these systems contain FTI. As part of this, the agency shall authorize, document, and monitor all device access to organizational information systems.		
AC20	PUBLICATION 1075 GUIDANCE: Agencies must develop policies for authorized individuals to access the information systems from an external system, such as access allowed from an alternate work site. This policy shall address the authorizations allowed to transmit, store, and/or process FTI. As part of this, the agency shall authorize, document, and monitor all access to organizational		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		information systems, where these systems contain FTI.		
8.16	TECHNICAL SECURITY CONTROLS			
	CONTROL FAMILY: AUDIT AND ACCOUNTABILITY			
	AU1	PUBLICATION 1075 GUIDANCE: Audit and accountability policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing audit and accountability security controls. Such audit and accountability security controls include auditable events; content of audit records; audit storage capacity; audit processing; audit monitoring, analysis and reporting; time stamps; protecting audit information and audit retention.		
	AU2	PUBLICATION 1075 GUIDANCE: The information system must generate audit records for all security-relevant events, including all security and system administrator accesses. An example of an audit activity is reviewing the administrator actions whenever security or system controls may be modified to ensure that all actions are authorized.		
	AU3	PUBLICATION 1075 GUIDANCE: Security-relevant events must enable the detection of unauthorized access to FTI data. System and/or security administrator processes will include all authentication processes to access the system, for both operating system and application-level events. Audit logs must enable tracking activities taking place on the system.		
	AU4	PUBLICATION 1075 GUIDANCE: Agencies must configure the information system to allocate sufficient audit record storage capacity to record all necessary auditable items.		
	AU5	PUBLICATION 1075 GUIDANCE: The information system shall alert appropriate organizational officials in the event of an audit processing failure and takes the additional actions.		
	AU6	PUBLICATION 1075 GUIDANCE: Agencies must routinely review audit records for indications of unusual activities, suspicious activities or suspected violations,		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		and report findings to appropriate officials for prompt resolution.		
	AU7	PUBLICATION 1075 GUIDANCE: To enable review of audit records, the information system provides an audit reduction and report generation capability.		
	AU8	PUBLICATION 1075 GUIDANCE: The information system shall provide date and time stamps for use in audit record generation.		
	AU9	PUBLICATION 1075 GUIDANCE: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
	AU11	PUBLICATION 1075 GUIDANCE: To support the audit of activities, all agencies must ensure that audit information is archived for six years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.		
8.17	TECHNICAL SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION			
	SC1	PUBLICATION 1075 GUIDANCE: System and communications policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing effective system and communications.		
	SC2	PUBLICATION 1075 GUIDANCE: The information system shall separate front end interface from the back end processing and data storage.		
	SC4	PUBLICATION 1075 GUIDANCE: The information system shall prevent unauthorized and unintended information transfer via shared system resources.		
	SC7	PUBLICATION 1075 GUIDANCE: The information system shall be configured to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.		
	SC9	PUBLICATION 1075 GUIDANCE: The information system must protect the confidentiality of FTI during electronic		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		transmission.		
	SC10	PUBLICATION 1075 GUIDANCE: Whenever there is a network connection, the information system shall terminate the network connection at the end of a session or after no more than fifteen minutes of inactivity.		
	SC12	PUBLICATION 1075 GUIDANCE: When Public Key Infrastructure (PKI) is used, the agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.		
	SC13	PUBLICATION 1075 GUIDANCE: When cryptography (encryption) is employed within the information system, the system must perform all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation. Cryptographic data transmissions are ciphered and consequently unreadable until deciphered by the recipient.		
	SC15	PUBLICATION 1075 GUIDANCE: The information system shall prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. Collaborative mechanisms include cameras and microphones that may be attached to the information system. Users must be notified if there are collaborative devices connected to the system.		
	SC17	PUBLICATION 1075 GUIDANCE: The agency shall establish PKI policies and practices, as necessary.		
	SC18	PUBLICATION 1075 GUIDANCE: The agency shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously. All mobile code must be authorized by the agency official.		
	SC19	PUBLICATION 1075 GUIDANCE: The agency shall establish, document and control usage restrictions and		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		implementation guidance for Voice over Internet Protocol (VoIP) technologies.		
	SC23	PUBLICATION 1075 GUIDANCE: The information system shall provide mechanisms to protect the authenticity of communications sessions.		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

8.18	DATA WAREHOUSE ADDITIONAL COMPUTER SECURITY CONTROLS Note: These controls are only applicable if the Data Warehouse is implemented in the computer system(s) that store, transmit, or process FTI.		
DW-RA	PUBLICATION 1075 GUIDANCE: The agency shall have a Risk Management Program in place to ensure each program is assessed for risk. Risks of the data warehousing environments shall be assessed. Any risk documents shall identify and document all vulnerabilities, associated with the Data Warehousing environment.		
DW-PL	PUBLICATION 1075 GUIDANCE: A Security Plan shall be in place to address organizational policies, security testing, rules of behavior, contingency plans, architecture/network diagrams, and requirements for security reviews. While the plan will provide planning guidelines, this will not replace requirements documents, which contain specific details and procedures for security operations. Policies and procedures are required to define how activities and day-to-day procedures will occur. This will contain the specific policies, relevant for all of the security disciplines covered in this document. As this relates to data warehousing, any Data Warehousing documents can be integrated into overall security procedures. A section shall be dedicated to data warehouses to define the controls specific to that environment. Develop policies and procedures to document all existing business processes. Ensure that roles are identified for the organization, regarding the specific roles being created and the responsibilities for these roles. Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing. Define how "legacy system data" will be brought into the data warehouse and how the legacy data		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		that is FTI will be cleansed for the ETL transformation process. The policy shall ensure that FTI will not be subject to Public Disclosure. Only clients or end users can query FTI data with a concrete "need to know".		
	DW-SA	PUBLICATION 1075 GUIDANCE: Acquisition security needs to be explored. As FTI is used within data warehousing environments, it will be important that the services and acquisitions have adequate security in place, including blocking information to contractors, where these contractors are not authorized to access FTI.		
	DW-CA	PUBLICATION 1075 GUIDANCE: Certification, accreditation, and security and risk assessments are accepted best practices used to ensure that appropriate levels of control exist, are being managed and are compliant with all Federal and State laws or statutes. State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in NIST SP 800- 53, February 2005. The process or policy must contain the methodology being used by the State or local agency to inform management, define accountability and address known security vulnerabilities. Risk assessments should follow the guidelines provided in NIST Publication 800-30 Risk Management Guide for Information Technology Systems, July 2002.		
	DW-PS	PUBLICATION 1075 GUIDANCE: Personnel clearances may vary from agency to agency. As a rule, personnel with access to FTI shall have a completed background investigation. In addition, when a staff member has administrator access to access the entire set of FTI records, additional background checks may be determined necessary. All staff interacting with DW and DM resources are subject to background investigations in order to ensure their trustworthiness, suitability, and work role need-to-know. Access to these resources must be authorized by operational		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	supervisors, granted by the resource owners, and audited by internal security auditors.		
DW-CP	<p>PUBLICATION 1075 GUIDANCE: On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. By using new technologies, agencies will ensure the data being provided is reliable. As necessary, based upon risk and cost, these tools shall be implemented. Both incremental and special purpose data back-up procedures are affected, accompanied by off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy, and are tested and verified. Though already addressed in the Publication 1075, this needs to be evaluated to ensure that all data resources are synchronized and restored to allow recreation of the data to take place.</p>		
DW-CM	<p>PUBLICATION 1075 GUIDANCE: The agency shall have a process and documentation to identify and analyze how existing FTI is used and how FTI is queried or targeted by end users. FTI parts of the system shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. During the life cycle of the DW, on-line and architectural adjustments and changes will occur. The agency shall document these changes and assure that FTI is always secured from unauthorized access or disclosure.</p>		
DW-MP	<p>PUBLICATION 1075 GUIDANCE: The agency shall have policy and procedures in place describing the Cleansing Process at the staging area and how the ETL process cleanses the FTI when it is extracted, transformed and loaded. Additionally, describe the process of object re-use once FTI is replaced from data sets. IRS requires all FTI is removed by a random overwrite software program.</p>		
DW-IR	<p>PUBLICATION 1075 GUIDANCE:</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	Intrusion detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data.		
DW-AT	<p>PUBLICATION 1075 GUIDANCE: The agency shall have a “training program” in place that will include how FTI security requirements will be communicated for end users. Training shall be user specific to ensure all personnel receive appropriate training for a particular job, such as training required for administrators or auditors.</p>		
DW-IA	<p>PUBLICATION 1075 GUIDANCE: The agency shall configure the web services to be authenticated before access is granted to users via an authentication server. Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure only authorized personnel have access to FTI information. Authentication shall be required both at the operating system level and at the application level, when accessing the data warehousing environment.</p>		
DW-AC	<p>PUBLICATION 1075 GUIDANCE: Access to systems shall be granted based upon the need to perform job functions. Agencies shall identify which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure only authorized personnel have access to the areas containing FTI.</p> <p>The agency shall have security controls in place that include preventative measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know there is an attack occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations.</p> <p>Within the DW, the agency shall protect FTI</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

as sensitive data and be granted access to FTI for the aspects of their job responsibility. The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job. The agency shall set up access controls in their DW based on personnel clearances. Access controls in a data warehouse are generally classified as 1) General Users; 2) Limited Access Users; and 3) Unlimited Access Users. FTI shall always fall into the Limited Access Users category.

All FTI shall have an owner assigned so that there is responsibility and accountability in protecting FTI. Typically, this role will be assigned to a management official such as an accrediting authority.

The agency shall configure control files and datasets to enable the data owner to analyze and review both authorized and unauthorized accesses.

The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be done at the authentication server.

Web-enabled application software shall:

1. Prohibit generic meta-characters from being present in input data
2. Have all database queries constructed with parameterized stored procedures to prevent SQL injection
3. Protect any variable used in scripts to prevent direct OS commands attacks
4. Have all comments removed for any code passed to the browser
5. Not allow users to see any debugging information on the client, and
6. Be checked before production deployment to ensure all sample, test and unused files have been removed from the production system.

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	<p>DW-AU</p>	<p>PUBLICATION 1075 GUIDANCE: The agency shall ensure that audit reports are created and reviewed for data warehousing- related access attempts. A data warehouse must capture all changes made to data, including: additions, modifications, or deletions. If a query is submitted, the audit log must identify the actual query being performed, the originator of the query, and relevant time/stamp information. For example, if a query is made to determine the number of people making over \$50,000, by John Doe, the audit log would store the fact that John Doe made a query to determine the people who made over \$50,000. The results of the query are not as significant as the types of query being performed.</p>		
	<p>DW-SC</p>	<p>PUBLICATION 1075 GUIDANCE: Whenever FTI is located on both production and test environments, these environments will be segregated. This is especially important in the development stages of the data warehouse.</p> <p>All Internet transmissions will be encrypted using HTTPS protocol utilizing Secure Sockets Layer (SSL) encryption based on a certificate containing a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This will allow information to be protected between the server and the workstation. During the Extract, Transform and Load stages of data entering a warehouse, data is at its highest risk. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption, i.e., from workstation to point of data.</p> <p>Web server(s) that receive online transactions shall be configured in a “Demilitarized Zone” (DMZ) in order to receive external transmissions but still have some measure of protection against unauthorized intrusion.</p> <p>Application server(s) and database server(s)</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		<p>shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers.</p> <p>Transaction data shall be “swept” from the web server(s) at frequent intervals consistent with good system performance, and removed to a secured server behind the firewalls, to minimize the risk that these transactions could be destroyed or altered by intrusion.</p> <p>Anti-virus software shall be installed and maintained with current updates on all servers and clients that contain tax data.</p> <p>For critical online resources, redundant systems shall be employed with automatic failover capability.</p>		
8.19	ADDITIONAL COMPUTER SECURITY CONTROLS - TRANSMITTING FTI			
	<i>ADT1</i>	<p>PUBLICATION 1075 GUIDANCE: All FTI data in transit must be encrypted, when moving across a Wide Area Network (WAN). Generally, FTI transmitted within the Local Area Network (LAN) should be encrypted. If encryption is not used, the agency must use other compensating mechanisms (e.g., switched vLAN technology, fiber optic medium, etc.) to ensure that FTI is not accessible to unauthorized users.</p>		
	<i>ADT2</i>	<p>PUBLICATION 1075 GUIDANCE: Unencrypted cable circuits of copper or fiber optics is an acceptable means of transmitting FTI. Measures are to be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. Additional precautions should be taken to protect the cable, (e.g., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms, and switching centers). In instances where encryption is not used, the agency must ensure that all wiring, conduits, and cabling</p>		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

		are within the control of agency personnel and that access to routers and network monitors are strictly controlled.		
8.20	ADDITIONAL COMPUTER SECURITY CONTROLS - REMOTE ACCESS			
	<i>ADR1</i>	PUBLICATION 1075 GUIDANCE: Authentication is provided through ID and password encryption for use over public telephone lines.		
	<i>ADR2</i>	PUBLICATION 1075 GUIDANCE: Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.		
	<i>ADR3</i>	PUBLICATION 1075 GUIDANCE: Standard access is provided through a toll-free number and through local telephone numbers to local data facilities. Both access methods (toll free and local numbers) require a special (encrypted) modem and/or Virtual Private Network (VPN) for every workstation and a smart card (microprocessor) for every user. Smart cards should have both identification and authentication features and should provide data encryption as well. Two-factor authentication is recommended whenever FTI is being accessed from an alternate work location.		
8.21	ADDITIONAL COMPUTER SECURITY CONTROLS - ELECTRONIC MAIL			
	<i>ADE1</i>	PUBLICATION 1075 GUIDANCE: Do not send FTI unencrypted in any email messages. Messages containing FTI must be attached and encrypted. Ensure that all messages sent are to the proper address. Employees should log off the computer when away from the area.		
8.22	ADDITIONAL COMPUTER SECURITY CONTROLS - FACSIMILE MAIL (FAX)			
	<i>ADF1</i>	PUBLICATION 1075 GUIDANCE: Have a trusted staff member at both the sending and receiving fax machines. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI. Place fax machines in a secured area. Include a cover sheet on fax transmissions that explicitly provides		

[State and Agency Name e.g. California Child Support] Safeguard Procedures Report (SPR) Analysis

	<p>guidance to the recipient, which includes: A notification of the sensitivity of the data and the need for protection and a notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.</p>		
<i>9. Agency Disclosure Awareness Program</i>			
<p>9.1</p>	<p><i>Is there a formal FTI awareness program developed and documented?</i></p> <p>Note: <i>Each agency receiving FTI should have an awareness program that annually notifies all employees having access to FTI of the confidentiality provisions of the IRC, a definition of what returns and what return information is, and the civil and criminal sanctions for unauthorized inspection or disclosure.</i></p>		

EXHIBIT 5

IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION.

(a) IN GENERAL.-

(1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES.-If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF UNITED STATES.-If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) EXCEPTIONS.-No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) DAMAGES.-In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of-

(1) the greater of-

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of-

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) PERIOD FOR BRINGING ACTION.-Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard

to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) NOTIFICATION OF UNLAWFUL INSPECTION AND DISCLOSURE.-If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of-

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or

(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) DEFINITIONS.-For purposes of this section, the terms "inspect", "inspection", "return" and "return information" have the respective meanings given such terms by section 6103(b).

(g) EXTENSION TO INFORMATION OBTAINED UNDER SECTION 3406.-For purposes of this section-

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

County Certification Letter

I certify that all employees having FTI access have received annual training. Employees have signed certification that they have read and understand the civil penalties associated with unauthorized disclosure of information provided to the California Department of Social Services by the Internal Revenue Service. These Employee certifications will remain on file within the County for a period of three years.

Signature

Title

Date

Please Print Name

County

Please mail this annually, no later than September 1st to:

CDSS
744 P Street MS 19-26
Attn: IRS Coordinator
Sacramento, CA 95814

II. CRIMINAL/CIVIL SANCTIONS:

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

EXHIBIT 7

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

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

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (6) All computer systems processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.
- (7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.
- (10) (Include any additional safeguards that may be appropriate.)

Sub-Contractor Certification Letter

If you come into contact with confidential (names, address, date of birth, etc.) Federal Tax Information (FTI) and distribute or disclose such information you could be found in violation of the Internal Revenue Code Section 7213 & 7431 with consequences of a felony punishable by a fine of up to \$5,000, or imprisonment up to five years, or both, together with the cost of prosecution.

I certify that I have read and understand the consequences (criminal\civil) of revealing confidential information as listed in Exhibit 5 of the IRS Publication 1075.

Signature	Title	Date
-----------	-------	------

Please Print Name	Company
-------------------	---------

Please mail this annually, no later than September 1st to:

CDSS
744 P Street MS 19-26
Attn: IRS Coordinator
Sacramento, CA 95814