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

CDSS
WILL LIGHTBOURNE
DIRECTOR

EDMUND G. BROWN JR.
GOVERNOR

August 14, 2015

ALL-COUNTY LETTER NO. 15-56

REASON FOR THIS TRANSMITTAL

[ ] State Law Change
[ ] Federal Law or Regulation Change
[ ] Court Order
[ ] Clarification Requested by One or More Counties
[X] Initiated by CDSS

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY INCOME AND ELIGIBILITY VERIFICATION SYSTEM COORDINATORS
ALL CALWORKS PROGRAM SPECIALISTS
ALL CALFRESH PROGRAM SPECIALISTS
ALL COUNTY SPECIAL INVESTIGATIVE UNIT CHIEFS
ALL CONSORTIA PROGRAM MANAGERS

SUBJECT: INFORMATION SECURITY INCIDENT REPORTING PROTOCOL FOR FEDERAL TAX INFORMATION AND PERSONALLY IDENTIFYING INFORMATION

REFERENCES: Internal Revenue Code Section 6103, Internal Revenue Service Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies (October 2014), Social Security Act Public Law 98-369 Section 1137 (42 U.S.C. 1320b–7), 45 Code of Federal Regulations Part 205.55, United States Code Title 26 Section 6103.

The purpose of this All County Letter (ACL) is to provide instructions to county welfare departments (CWDs) regarding when and how to report information security incidents to the appropriate federal agencies involving federal tax information (FTI) or federal personally identifying information (PII) contained in certain Income and Eligibility Verification System (IEVS) match reports. These instructions apply to all FTI and the Social Security Administration (SSA) PII referenced in this ACL and includes both paper and electronic data.

Both the Internal Revenue Service (IRS) and the SSA require agencies that receive, store, process, or transmit FTI to develop, document, and disseminate policy and procedures covering incident response for FTI. Additionally, the SSA requires agencies that receive PII to establish a similar incident response process. CWDs may use this ACL in addition to IRS Pub 1075 as their internal FTI Incident Response Policy or,

CWDs may develop their own FTI Incident Response Policy based on the instructions and guidelines provided in this ACL. In addition, to meet the IRS' requirements, the CWD policy or procedure must specifically state that its scope covers "federal tax information."

DEFINITIONS

Authorized persons are employees of the CWD who meet the following criteria:

- Need to access data in order to perform their job duties.
- Have completed all required security training relevant to the data.
- Have completed all required security certifications relevant to the data which are on file and available for review by an outside agency.

FTI is data originally sourced from a federal tax return (including attachments) that the IRS then provides to human services agencies under IRC §6103(l)(7). It is important to note that when the same information is provided by the taxpayer to the CWD, it is *not* FTI. For example, if Jane Doe provides her federal tax return, this data is not FTI. When the IRS provides data from Jane Doe's federal tax return, this data is FTI.

PII is a combination of personal information such as a person's name with social security number (SSN) or date of birth (DOB). PII can be used to identify an individual person. For example, "Jane Doe" is not PII, but "Jane Doe DOB 1/1/1980" is PII. Even if the same information is self-reported by the individual, the information is PII because it can be used to identify the individual.

FTI may or may not be PII. For example, the name of the employer or banking institution from a Beneficiary Earning Exchange Record (BEER) or IRS Asset abstract is not PII, but is FTI.

GENERAL REPORTING GUIDELINES

These guidelines apply to *all* forms of FTI and SSA PII data. If a document or file containing FTI or SSA PII is involved in an information security incident, the information incident must be reported to the proper federal agencies.

CWDs are required to report an incident involving any FTI or SSA PII anytime the information:

- becomes missing or unaccounted for; (e.g., records show a paper abstract was removed from a secured room to be worked on but was not returned);
- has been accessed by unauthorized person(s) (e.g., an unauthorized staff person opened a file that was saved in an unsecured folder);

- has been disclosed to unauthorized person(s) (e.g., two authorized staff discuss FTI from a report in an open area where unauthorized staff can overhear); or
- the security measures in place to protect the FTI or SSA PII were breached or are suspected of having been breached (e.g. the door handle of a secured room is broken; an encryption program does not adequately encrypt files sent by email).

If the CWD is uncertain whether the incident is an information security incident that must be reported, please contact the California Department of Social Services (CDSS) Fraud Bureau (see Attachment 3).

CWDs receive FTI via the following IEVS Reports:
- Annual IRS Asset Match (paper only)
- Monthly Beneficiary Earnings Exchange Record (BEER) Match (paper only)

Incidents containing FTI must be reported to the IRS Office of Safeguards and the Treasury Inspector General for Tax Administration (TIGTA). See contact information in Attachment 3.

CWDs receive SSA PII via the following IEVS Reports:
- BEER Match (paper only)
- Payment Verification System (PVS) Match (electronic only)
- Integrated Earning Clearance/Fraud Detection System (IFD) Match (electronic only)
- Deceased Persons Match (DPM; paper only) and
- Nationwide Prisoner Match (NPM; paper or electronic)

Incidents involving SSA PII must be reported to the Social Security Administration. See contact information in Attachment 3.

The IRS and TIGTA require notification of incident information **within 24 hours of discovery** of the incident, including weekends and holidays. The SSA requires notification within **one (1) hour of discovery**. ("Discovery" occurs when an individual becomes aware of the incident.) Although there is no hierarchy for reporting information incidents, if there is a security incident involving both FTI and SSA PII, it will be necessary to report to the SSA first to meet its one-hour reporting requirement.

The individual making the observation or receiving information of an incident is required to report the incident using a specified format or template. The individual should be prepared to respond to additional requests for information or follow-up from IRS, SSA, TIGTA, and/or CDSS Fraud Bureau.

During normal business hours (Monday through Friday, 8am to 5pm), CWDs should contact the CDSS Fraud Bureau (see Attachment 3) and provide all the information requested in Attachments 1 and/or 2. When reporting to CDSS Fraud Bureau, please

report immediately in order for CDSS Fraud Bureau to meet the one-hour and 24-hour reporting timeframes. The CDSS Fraud Bureau will complete the data incident report(s) and submit to the applicable federal agency or agencies, as well as provide a copy to the CWD contact which provided the information in the Attachment 1 and/or Attachment 2. However, in the event the incident is discovered outside of normal State business hours, such as nights, weekends, or holidays, and there is insufficient time to contact the CDSS Fraud Bureau and meet the applicable required reporting time, the CWD must contact the federal agency or agencies directly. In those situations, please include the CDSS Fraud Bureau in all communications or meetings with the federal agency or agencies throughout the information incident response process.

To prevent further disclosure of FTI, never include FTI in any incident reports, emails, faxes, or other communications used in the information incident response process.

SPECIFIC REPORTING REQUIREMENTS IF AN INCIDENT IS DISCOVERED OUTSIDE OF STATE BUSINESS HOURS

FTI Incident – Report to the IRS Office of Safeguards (Applicable to BEER and IRS Matches Only)

The IRS Office of Safeguards requires agencies to submit incident reports by email to safeguardreports@irs.gov. The initial notification must be made no later than 24 hours after discovery of the incident. Attachment 3 provides the contact information. A CWD must use the IRS Office of Safeguards Data Incident Report PI 2 (6/15) (see Attachment 1). This form is also referred to as “IRS DIR (PI 2).” The IRS DIR (PI 2) can be completed and attached to an email or the information can be included in the body of the email.

When reporting directly, use the term “Data Incident Report” in the subject line of the email and mark the email as “URGENT” or of “High Importance.” This will help the IRS respond rapidly to the incident.

The IRS will contact the person listed on the Attachment 1 IRS DIR (PI 2) and provide the contact with an IRS incident number. All communication relating to the incident must reference the IRS incident number. The IRS will also request a follow-up meeting to discuss the incident. Depending on the complexity of the incident, the IRS may or may not schedule further meetings in order to close the incident. In the event missing or data that is unaccounted for is found, the CWD must notify CDSS Fraud Bureau so that all agencies originally notified of the incident can be updated.

Note, the notification of the breach of data to the impacted individuals is based upon the CWD’s internal policy. The CWD must inform the IRS Office of Safeguards of notification activities undertaken before the notifications are released to the impacted individuals. In addition, the CWD must inform the IRS Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

FTI Incident – Report to the TIGTA (Applicable to BEER and IRS Asset Matches Only)

To meet the 24-hour reporting requirement, the TIGTA provides direct contact phone numbers. Please see Attachment 3 for contact information. A TIGTA Special Agent will request a meeting with the reporting agency in order to gather all relevant facts for his or her investigation of the incident. The TIGTA Special Agent may request a brief listing of the facts of the incident. Please include the CDSS Fraud Bureau in all communications or meetings with agencies outside the CWD throughout the information incident response process.

TIGTA is authorized to investigate FTI incidents only. Because a federal tax return or return information provided by the taxpayer is not FTI, the CWD will need to specify to TIGTA that the incident affects FTI data. CWDs will need to specify if the incident is from: 1) IRS Asset match data which is provided through the IRS Disclosure to Federal, State, and Local Agencies (DIFSLA) program; or 2) BEER match data which is provided through the SSA Beneficiary and Earnings Data Exchange (BENDEX) system. The IRS and SSA data through the DIFSLA and BENDEX processes are under the authority of 26 U.S.C. §6103(l)(7), 45 CFR Part 205.55, and Section 1137 of the Social Security Act (42 U.S.C. 1320b–7). In the event the TIGTA Special Agent asks why the data is FTI, providing a copy of this ACL or the above-listed reference information will meet this requirement.

The TIGTA Special Agent may also request copies of the following documents and other information:

- IRS Incident number
- The IRS DIR (PI 2) submitted to the IRS Office of Safeguards
- The email used to notify the IRS Office of Safeguards of the incident
- Acronym list for data, programs, units, departments, etc.
- Diagram or a brief description of the flow of the data from the IRS or SSA to the CWD

The TIGTA Special Agent may need to examine the physical safeguards in place in the event of a breach of physical safeguards, e.g., broken lock or door handle, stolen key card, jammed windows, etc.

The TIGTA Special Agent will provide a report of his or her investigation of the incident to the IRS Office of Safeguards. The IRS is responsible for closing the incident and contacting the reporting agency. If the CDSS Fraud Bureau reports the incident on

behalf of the CWD, the Fraud Bureau will inform the CWD of the incident response status or a request for information or clarification of the facts.

Based upon the analysis of the incident by the IRS and TIGTA, the IRS may require the CWD to modify security policies, procedures, or controls protecting FTI in the CWD's possession. The IRS will coordinate with CDSS Fraud Bureau and the CWD to ensure appropriate follow-up actions have been completed to ensure continued protection of FTI.

PII Incident – Report to the SSA (Applicable to BEER, NPM, PVS, IFD, and DPM Only)

CWDs must use the SSA Data Incident Report PI 1 (6/15) (see Attachment 2). This form is also referred to as "SSA DIR (PI 1)." The SSA DIR (PI 1) can be completed and attached to an email or the information can be included in the body of the email. If the exact number of records is not known at the time of the initial report, be prepared to provide an approximate number.

The SSA Regional Office will contact the individual listed on the completed SSA DIR (PI 1) to clarify any questions and discuss next steps. These next steps may include but are not limited to: providing a template of data involved, providing an update of notifications to individuals whose PII was involved, planned or implemented remediation, and current incident response protocols. If the incident involves BEER data, the SSA may also request the IRS' incident number for reference.

Please note that the IRS requires agencies to use IRS-approved encryption techniques when submitting DIRs by email. The encryption instructions also apply when sending SSA DIR (PI 1). See Attachment 5 for the encryption protocol.

CDSS is also providing a one-page summary of information (Quick View) to assist CWDs when reporting a security incident directly to the IRS, TIGTA or SSA. See Attachment 4 – IRS and SSA Information Incident Reporting Quick View.

You may also obtain blank forms from the CDSS Forms Management Unit at fmudss@dss.ca.gov or the webpage at http://www.dss.cahwnet.gov/cdssweb/FormsandPu_271.htm. Both the SSA DIR (PI 1) and the IRS DIR (PI 2) forms available at this link are camera-ready and fillable.

NOTE: Statewide Automated Welfare System (SAWS) case records must never include FTI. A separate ACL will be forthcoming to provide additional guidance regarding applicable restrictions.

If you have any questions regarding this letter, please contact Nancy Cronin, Fraud Analyst, at (916) 651-5007 or email her at Nancy.Cronin@dss.ca.gov.

Sincerely,

Original Document Signed by:

TODD R. BLAND
Deputy Director
Welfare to Work Division

Attachments

SSA DATA INCIDENT REPORT

Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information (PII)

1. Information about the individual making the report:

NAME:		
POSITION:		
STATE:	COUNTY AGENCY:	
PHONE NUMBERS:		
WORK:	CELL:	HOME/OTHER:
E-MAIL ADDRESS:		
CHECK ONE OF THE FOLLOWING:		
☐ Management Official	☐ Security Officer	☐ Non-Management

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

☐ Name ☐ Bank Account Info ☐ SSN ☐ Medical/Health Information
☐ Date of Birth ☐ Benefit Payment Info ☐ Place of Birth ☐ Mother's Maiden Name
☐ Address ☐ Other (describe):_____

3. How was the data physically stored, packaged and/or contained?

☐ Paper or ☐ Electronic? (check one and continue below):

If Electronic, what type of device?

☐ Laptop ☐ Tablet ☐ Backup Tape ☐ Smart Phone
☐ Workstation ☐ Server ☐ CD/DVD Smart Phone Phone #_____
☐ Hard Drive ☐ Floppy Disk ☐ USB Drive
☐ Other (describe):_____

Additional Questions if Electronic:

a. Was the device encrypted? ☐ Yes ☐ No ☐ Not Sure
b. Was the device password protected? ☐ Yes ☐ No ☐ Not Sure
c. If a laptop or tablet, was a VPN SmartCard lost? ☐ Yes ☐ No ☐ Not Sure
d. If laptop, powerstate when lost? ☐ Off ☐ Sleep ☐ Hibernate ☐ Not Sure

Cardholder's Name:_____

Cardholder's SSA logon PIN:_____

Hardware Make/Model:_____

Hardware Serial Number:_____

Additional Questions if Paper:

a. Was the information in a locked briefcase? ☐ Yes ☐ No ☐ Not Sure
b. Was the information in a locked cabinet or drawer? ☐ Yes ☐ No ☐ Not Sure
c. Was the information in a locked vehicle trunk? ☐ Yes ☐ No ☐ Not Sure
d. Was the information redacted? ☐ Yes ☐ No ☐ Not Sure
e. Other circumstances:_____

4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report (as listed in #1), information about this employee/contractor:

NAME:		
POSITION:		
STATE:	COUNTY AGENCY:	
PHONE NUMBERS:		
WORK:	CELL:	HOME/OTHER:
E-MAIL ADDRESS:		

5. Circumstances of the loss:

a. When was it lost/stolen? _____

b. Brief description of how the loss/theft occurred:_____

c. When was it reported to SSA management official (date and time)?_____

6. Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)

_____

_____

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed		
Federal Protective Service	☐ Yes ☐ No	Report Number_____
Local Police	☐ Yes ☐ No	Report Number_____
OIG	☐ Yes ☐ No	Report Number_____
SSA-3114 (Incident Alert)	☐ Yes ☐ No	
SSA-342 (Report of Survey)	☐ Yes ☐ No	
Security Assessments and Funded Enhancements (SAFE)	☐ Yes ☐ No	

Other (describe) _____

_____

8. Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):

9. Describe how the incident or potential incident was discovered, including the date and time of discovery:

IRS OFFICE OF SAFEGUARDS
DATA INCIDENT REPORT (for federal tax information only)

Contact Information		
AGENCY NAME:	AGENCY ADDRESS:	
CONTACT NAME:	PHONE #:	EMAIL ADDRESS:

Incident Information	
DATE INCIDENT *OCCURRED*:	DATE INCIDENT *DISCOVERED*:
TIME INCIDENT *OCCURRED*:	TIME INCIDENT *DISCOVERED*:
DESCRIPTION OF INCIDENT DISCOVERY:	ADDRESS WHERE INCIDENT OCCURRED:
DESCRIPTION OF INCIDENT:	
DATA INVOLVED (INCLUDE SPECIFIC ELEMENTS IF KNOWN)	# OF FTI RECORDS AFFECTED:
SPECIFIC TECHNOLOGY INVOLVED (E.G., LAPTOP, SERVER, MAINFRAME)	

Incident Response Information (Safeguards Use Only)	
REPORT DATE:	REPORT TIME:

Attachment 3

INFORMATION SECURITY INCIDENT REPORTING CONTACT INFORMATION

For SSA and IRS Data

CDSS Fraud Bureau
744 P Street, MS 9-11-26
Sacramento, CA 95814
Phone: (916) 653-1826
Fax: (916) 651-5009
Email: fraudprevention@dss.ca.gov

Internal Revenue Services (IRS) Office of Safeguards
Email: safeguardreports@irs.gov

Treasury Inspector General for Tax Administration (TIGTA)
Special Agent-in-Charge
San Francisco Regional Office
Local Office: (510) 637-2558
National Office: (800)589-3718
Mailing Address:
TIGTA
Ben Franklin Station
PO Box 589
Washington, DC 20044-0589

Social Security Administration (SSA) Regional Office
SF.CA.RO.Region.IX.Data.Exchange@ssa.gov
Phone: (510) 970-8243
Fax: (510) 970-8101

IRS and SSA Information Security Incident Reporting Quick View

In the event there is a security incident related to federal tax information (FTI) or Personal Identifying Information (PII), the CWD is required to report the incident to CDSS. If the incident occurs after hours, weekends or holidays, the CWD is required to report directly to the IRS or SSA. This quick view outlines the information needed to determine what type of data may have been disclosed, the source entity and how to report the incident.

This chart lists which agency provided the data to CDSS and if the data is FTI and/or PII.

Match	Agency	Data Type
IRS Asset	IRS	FTI and PII
BEER	SSA	FTI and PII
PVS	SSA	PII
IFD	SSA	PII
NPM	SSA	PII
DPM	SSA	PII

This chart lists the agencies that should be contacted in the event of a security incident involving the data.

Match	IRS	TIGTA	SSA
IRS Asset	Yes	Yes	No
BEER	Yes	Yes	Yes
PVS	No	No	Yes
IFD	No	No	Yes
NPM	No	No	Yes
DPM	No	No	Yes

This chart lists the methods for reporting information incidents to the agencies.
Remember: all emails and attachments used to report the incident must be encrypted

Agency	Form	Email	Fax	Telephone
CDSS	n/a	FraudPrevention@dss.ca.gov	(916) 651-5009	(916) 653-1826
IRS	IRS Data Incident Report (PI 2)	safeguardreports@irs.gov	n/a	n/a
TIGTA	n/a	n/a	n/a	California (510) 637-2558 National (800) 589-3718
SSA	SSA Data Incident Report (PI 1)	SF.CA.RO.Region.IX.Data.Exchange@ssa.gov	n/a	n/a

Please cc the CDSS in all your correspondence with the federal agencies.

Encryption Procedures

For Emailing Information Security Incident Reports to IRS and SSA

This procedure is provided as a resource in the event the CWD must email an IRS DIR (PI 2) to the IRS or an SSA DIR (PI 1) to the SSA. (Be sure to include the CDSS Fraud Bureau at FraudPrevention@dss.ca.gov.)

There are several types of utilities available for compressing and encrypting files. The IRS requires ".zip" file formats, which most (but not all) compression utilities support. We recommend using a strong 256-bit encryption key string, which is widely available in most modern compression utilities. Contact your information technology support staff for assistance installing or using a compression utility.

IRS Standards:

- ✓ Compress files in .zip or .zipx formats.
- ✓ Encrypt the compressed file using Advanced Encryption Standard (AES). (This is usually an option with compression utilities.)
- ✓ Ensure a strong password or pass phrase is used to encrypt the file. This can be done using a minimum of eight (8) characters and a mix of upper case, lower case, numbers, and special characters.
- ✓ Communicate the password or pass phrase to the recipient in a separate email or by a telephone call. Do not include the password or pass phrase in the same email containing the encrypted attachment.
- ✓ Do not include FTI or PII in the body or subject line of the email.

For FTI safeguard support, contact the CDSS Welfare Fraud Bureau at (916) 653-1826 or fraudprevention@dss.ca.gov, or visit the IRS' Safeguards web page.

Source: Pub 1075 section 7.1.2 Encryption Requirements