

September 9, 2019

CALIFORNIA DEPARTMENT OF SOCIAL SERVICES

EXECUTIVE SUMMARY

ALL COUNTY LETTER NO. 19-83

This ACL requires counties that have chosen to maintain and use electronic federal tax information (FTI) in a computer or computers to conduct regular audits of these computer systems and to report the results of these system audits to CDSS.



KIM JOHNSON
DIRECTOR

STATE OF CALIFORNIA—HEALTH AND HUMAN SERVICES AGENCY
DEPARTMENT OF SOCIAL SERVICES
744 P Street • Sacramento, CA 95814 • www.cdss.ca.gov



GAVIN NEWSOM
GOVERNOR

September 9, 2019

ALL COUNTY LETTER (ACL) NO. 19-83

TO: ALL COUNT WELFARE DIRECTORS
ALL COUNTY INFORMATION SYSTEM SECURITY OFFICERS
ALL COUNTY INCOME AND ELIGIBILITY VERIFICATION SYSTEM
COORDINATORS

SUBJECT: AUDIT REQUIREMENTS FOR SYSTEMS CONTAINING FEDERAL
TAX INFORMATION (FTI)

REFERENCE: [UNITED STATES CODE TITLE 26 - INTERNAL REVENUE CODE
SECTIONS 6103\(p\)\(4\) AND 6103\(l\)\(7\);
INTERNAL REVENUE SERVICE PUBLICATION 1075 "TAX
INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE
AND LOCAL AGENCIES" \("PUB 1075"\);
MANUAL OF POLICIES AND PROCEDURES SECTION 20-006](#)

This all county letter (ACL) provides guidance and requirements for electronic federal tax information (FTI) and county-level audits of systems containing electronic FTI.

The California Department of Social Services (CDSS) provides FTI to county welfare departments (CWDs) in the paper IRS Asset and Beneficiary Earnings Exchange Record (BEER) matches produced as part of the Income and Eligibility Verification System (IEVS). All documents and files containing FTI are subject to the audit requirements of the [IRS Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies \(Pub 1075\)](#). Several CWDs have opted to input FTI from their paper IRS Asset and BEER matches into electronic formats such as Access databases or Excel workbooks. The computers containing this electronic FTI are subject to the requirements of this ACL.

The CWDs are strongly discouraged from creating electronic FTI due to the vulnerability of electronic data and the challenges involved with securing FTI sufficient to meet [Pub 1075](#) requirements. The CWDs that have created electronic FTI are required to perform

audits of data systems that contain FTI and transmit the results of these audits to the CDSS. The challenges associated with securing networks can be reduced by using standalone computers that are not and cannot be connected to any other device or network system. However, these standalone computers are not exempt from meeting the requirements of this ACL and of [Pub 1075](#).

As a reminder, FTI must never be entered, processed, stored, or transmitted by data systems or devices that are not owned, operated, or maintained by the county. This includes, but is not limited to, the California Statewide Automated Welfare System or the California Welfare Information Network (known as “CalSAWS” and “CalWIN,” respectively) consortia systems. See [ACL 16-106 Re-Disclosure Restriction of Federal Tax Information to Contractors](#), dated December 23, 2016, for more information.

Background

In January 2017, the IRS Office of Safeguards reviewed the CDSS and two CWD offices to evaluate the methods utilized by the CDSS and CWDs to protect FTI against loss, breach or misuse, and prevent unauthorized disclosure or access by individuals without a need-to-know. The IRS found that the CDSS and CWDs lack a policy and procedure for the CWDs to conduct regular audits of systems that contain FTI and provide the results of these audits to the CDSS. The IRS requires the CDSS to be aware of how CWDs use and secure electronic FTI. The CDSS IEVS Review Analysts inspect physical safeguards during their reviews but do not conduct in-depth inspections or audits of computers or systems that contain, transmit, or utilize FTI. For this reason, this ACL is necessary to provide those CWDs with electronic FTI with the minimum system audits and reporting requirements.

Scope

This ACL is limited to the auditing of county-owned and operated data systems that process, store, or otherwise contain FTI and the audits conducted of these systems. This ACL does not cover non-FTI information systems, nor does this ACL supersede the requirements of [Pub 1075](#).

Requirement and Support Resources

In addition to [Pub 1075](#), counties can obtain support material from the National Institutes of Standards and Technology (NIST) Special Publications (SP) and the IRS Office of Safeguards website. These materials include, but are not limited to, [Safeguard Computer Security Evaluation Matrices \(SCSEM\)](#), the industry standard compliance and vulnerability [assessment tool Nessus](#), and technical assistance by topic. The [NIST SPs](#) can be accessed at the [Computer Security Resource Center](#). Audit-related NIST information can be found at the [NIST Audit and Accountability Control Family](#) page.

CWD Audit and Accountability Policies and Procedures

Any county system that contains FTI must be audited per [Pub 1075](#), Section 9.3.3 Audit and Accountability. The CWD must develop and update policies and procedures for conducting audits of county systems that contain FTI. These audit and accountability policies must be reviewed and updated as needed or every three years at a minimum. The CWD procedures for conducting audits must be reviewed and updated as needed or, at a minimum, once a year.

Audit Events

An event is any observable occurrence in an organizational information system. Audit events are identified as those events which are significant and relevant to the security of information systems and the environments in which those systems operate to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, personal identity verification credential usage, or third-party credential usage. In determining the set of auditable events, counties should consider the auditing appropriate for each of the security controls to be implemented.

Per [Pub 1075](#) Section 9.3.3.2, Audit Events, "Security-relevant events must enable the detection of unauthorized access to FTI data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of FTI by each unique user."

The county must determine that the information system is capable, at a minimum, of auditing the following event types:

1. Log onto system.
2. Log off from system.
3. Change of password.
4. All system administrator commands, while logged on as system administrator,
5. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS),
6. Creation or modification of super-user groups,
7. Subset of security administrator commands, while logged on in the security administrator role.
8. Subset of system administrator commands, while logged on in the user role.
9. Clearing of the audit log file.
10. Startup and shutdown of audit functions.
11. Use of identification and authentication mechanisms (e.g., user ID and password).
12. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su).
13. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system.
14. Changes made to an application or database by a batch file.

15. Application-critical record changes.
16. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility).
17. All system and data interactions concerning FTI.
18. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website.

The county must also:

- Coordinate the security audit function with other county divisions requiring audit- related information to enhance mutual support and to help guide the selection of auditable events.
- Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
- Review and update the audited events annually at a minimum.

Audits must be conducted at the operating system, software, and database levels. Software and platforms differ in audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific IRS Office of Safeguards SCSEM. The SCSEMs are available on the IRS Office of Safeguards website.

Audit Record Content Elements

The information system must generate audit records containing sufficient details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected.

System audits must include, at a minimum, the following data record elements:

- Type of event that occurred;
- When (date and time) the event occurred;
- Where the event occurred;
- The source of the event;
- The outcome of the event;
- The identity of any individuals or subjects associated with the event.

Storage Capacity and Audit Information Protection

Audit records must be stored for a minimum of seven (7) years. Counties must allot sufficient storage capacity to maintain audit records.

Audit records must be protected from unauthorized access, modification, and/or deletion. The county must authorize only the designated security administrator(s) or staff other than system and network administrator(s) with access to manage audit

functionality. The county must never allow system or network administrators to have the ability to modify or delete audit log entries.

Response to Audit Processing Failures

Audit processes may fail due to, for example, storage capacity being reached or exceeded, an audit mechanism failure, or errors in software or hardware. The information system should detect and respond to these failures. At a minimum, the system must:

- Alert designated county officials in the event of an audit processing failure.
- Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator.
- Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.

Audit Review, Analysis, and Information Incident Reporting

Counties must review and analyze information system audit records weekly, at a minimum, or more frequently at the county's discretion. These reviews should focus on indications of unusual activity related to possible unauthorized access to FTI.

Counties must report findings according to county and the CDSS policies. (See Transmitting Audit Reports to the CDSS section below.) If the finding involves a potential unauthorized disclosure of FTI, the county must report the suspected or actual unauthorized disclosure of FTI. See [ACL 15-56 Information Security Incident Reporting Protocol for Federal Tax Information and Personally Identifying Information](#), dated August 14, 2015, for more information.

Also, counties are encouraged, but not required, to identify events that *may* indicate a potential unauthorized access to FTI.

Proactive Auditing Methods to Detect Unauthorized Access to FTI

Below is a table of auditing methods counties may use to detect unauthorized access to FTI. The items listed in the table are not required.

Table - Proactive Auditing Methods

Method	Detection Criteria
Time of Day Access	Identify suspicious behavior by tracking FTI accesses outside normal business hours

Method	Detection Criteria
Name Searches	Detect potential unauthorized access by monitoring name searches (especially searches on the same last name as the employee)
Previous Accesses	Identify employee accesses to Social Security Numbers (SSNs) that the employee has accessed in the past but currently does not have a case assignment or need to access
Previous Accesses	Monitor the volume of accesses a person performs and compare them to past case assignment levels
Zip Code	Determine whether an employee is accessing taxpayers whose address of record is geographically close to the employee's home or work location (i.e., same building, zip code, block)
Restricted SSN	Monitor all SSNs associated with past employees' tax returns (e.g., self, spouse, children, businesses).

If the county implements proactive audit methods, the county would improve audit results by defining the frequency for updating individuals' information to keep it current.

Audit Reduction and Report Generation

Audit reduction is a process that manipulates collected audit information and organizes this information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities are not always generated from the same information system or from the same function that conducts auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records.

Counties must include an audit reduction and report generation capability within the audit process. The audit reduction and report generation must support on-demand audit reviews, analysis, and reporting requirements and after-the-fact investigations of security incidents. The audit reduction and report generation capability must not alter the original content or time ordering of audit records. (Time ordering means the correlation of time stamps in individual audit records to the time stamps of other audit records.)

Time Stamps

The county must ensure the information system:

- Uses internal system clocks to generate time stamps for audit records;

- Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT);
- Compares and synchronizes the internal information system clocks to an enterprise-wide authoritative time source. (Where possible, synchronize enterprise time source to an external source, e.g., [NIST](#), Naval Observatory).

Audit Generation

Audit records can be generated from many different information system components. Typically, an information system can audit more events than required to meet those listed in the Audit Events section above. Counties may choose to audit more events than those listed in Audit Events. Counties must ensure their information systems:

- Provide audit record generation capability for the auditable events defined in Audit Events section above;
- Allow designated county agency officials to select which auditable events are to be audited by specific components of the information system;
- Generate audit records for the events with the content defined in Audit Events section above.
- Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.
- Provide the capability for flexibility to change the auditing based on selected criteria within thresholds the county agency deems necessary.

Transmitting Audit Reports to the CDSS

The CDSS is required to be aware of county processes of information systems that contain, process, store, or transmit the FTI that the CDSS provides to counties and all FTI created from this FTI. For this reason, counties must transmit audit reports and analyses of audit reports to the CDSS annually at a minimum, or as needed to report incidents or potential incidents. Transmission of audit reports to the CDSS Program Integrity Bureau must use a secure method, for example, encrypted files or a secure file transfer process.

Audit reports submitted to the CDSS must include an analysis of the audit results and include the number of records. Annual audit reports must be submitted no later than August 31st and may be submitted by email to FraudPrevention@dss.ca.gov.

Requirements Timeframes Summary List

The following list provides the timeframes for requirements included in this ACL:

- Develop and implement a policy and procedures for conducting system audits by February 28, 2020. The CWDs must report their progress toward completion of this requirement on the Annual Internal Inspection – Safeguard Activity Report.
- Review and analyze information system audit records weekly.
- Submit audit reports and analyses to CDSS as needed to report incidents or potential incidents or annually by August 31st.
- Review and update procedures for conducting audits as needed or annually (minimum).
- Review and update audit and accountability policies as needed or every three (3) years (minimum).
- Store audit records for a minimum of seven (7) years.

If you have any questions, please contact the Fraud Bureau Safeguard Coordinator at (916) 651-1826 or FraudPrevention@dss.ca.gov.

Sincerely,

Original Document Signed By:

TODD R. BLAND
Assistant Director
Automation, Integrity, and Client Initiatives Branch