

March 26, 2018

ALL COUNTY LETTER NO. 18-37

TO: ALL COUNTY WELFARE DIRECTORS
ALL COUNTY SPECIAL INVESTIGATIVE UNIT CHIEFS
ALL COUNTY INCOME AND ELIGIBILITY VERIFICATION
SYSTEM COORDINATORS
ALL COUNTY CALIFORNIA WORK OPPORTUNITY AND
RESPONSIBILITY TO KIDS PROGRAM SPECIALISTS
ALL COUNTY CALFRESH PROGRAM SPECIALISTS

SUBJECT: SAFEGUARD REQUIREMENTS FOR VOICE OVER INTERNET
PROTOCOL AND FEDERAL TAX INFORMATION

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" \("PUB 1075"\)](#)
[NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
SPECIAL PUBLICATION 800-58 SECURITY CONSIDERATIONS
FOR VOICE OVER IP SYSTEMS](#)
[MANUAL OF POLICIES AND PROCEDURES SECTION 20-006](#)
[ACL 16-106 REDISCLOSURE OF FEDERAL TAX INFORMATION
TO CONTRACTORS](#)

The purpose of this all county letter (ACL) is to instruct county welfare departments (CWD) of the requirements for safeguarding federal tax information (FTI), specifically electronic FTI and the systems that receive, store, process, or transmit electronic FTI when used with Voice over Internet Protocol (VoIP). This ACL covers only the FTI provided by the California Department of Social Services (CDSS) in use with VoIP telephone systems.

Background

The Internal Revenue Service (IRS) and Social Security Administration (SSA) provide CDSS with FTI as part of the Income and Eligibility Verification System (IEVS) IRS Asset and Beneficiary Earnings Exchange Record (BEER) matches. Every three years the IRS and SSA conduct reviews to determine the adequacy of safeguards used by the CDSS and CWDs to secure FTI from loss, damage, breaches, and unauthorized access and/or disclosure. The January 2017 IRS Safeguard Review determined a number of findings related to the VoIP system at a CWD. The IRS and the SSA provide FTI to human services agencies under IRC section 6103(l)(7). See [Pub 1075](#) section 1.4 “Key Definitions” for more information.

“Federal tax information” is a term of art that refers specifically to data originally sourced from federal tax returns and provided by federal agencies under section 6103 of the Internal Revenue Code (IRC). Other data may be known as “FTI,” but not all FTI is subject to the safeguard requirements of [IRC section 6103\(p\)\(4\)](#). The FTI that the CDSS receives from the IRS and SSA under [IRC 6103\(l\)\(7\)](#) and provides to counties in the BEER and IRS Asset matches is subject to [IRC 6103\(p\)\(4\)](#) safeguards.

All VoIP systems convert analog audio signals into digital data packets that can be transmitted through networks, including the internet. (Certain types of video conferencing also use VoIP technology and systems.) Many CWDs have switched to VoIP because it is less expensive than analog Public Switched Telephone Network (PSTN) phone services. However, VoIP systems that carry FTI must be secured.

Scope

This ACL covers electronic FTI created from the FTI provided by CDSS by the use of VoIP technology and systems.

Requirements

This ACL focuses on the requirements outlined in the [IRS’ Publication 1075 Tax Information Security Guidelines for Federal, State, and Local Agencies](#) (“[Pub 1075](#)”) and detailed in the National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-58 Security Considerations for Voice over IP Systems](#). This ACL is not intended to supersede the requirements of the current version of [Pub 1075](#). This ACL is also not intended to provide all safeguard requirements for safeguarding FTI in relation to VoIP technology. Regardless of other factors, CWDs must adhere to the requirements contained in [Pub 1075](#) in relation to the FTI provided by CDSS or created from the FTI provided by CDSS.

Authorized employees of the CWD may disclose FTI only over landlines and/or VoIP systems that meet IRS requirements. If a CWD chooses to use a VoIP system in order to discuss FTI with a client, the CWD must meet, at a minimum, the following mandatory requirements:

- The VoIP traffic that contains FTI should be segmented off from non-VoIP.
- When FTI is in transit across the network (either Internet or the CWD's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode.
- VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in [Pub 1075](#) Section 4.0, "Secure Storage."
- Each system within the CWD's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements provided in [Pub 1075](#) and is subject to frequent vulnerability testing.
- VoIP-ready firewalls must be used to filter VoIP traffic on the network.
- Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter. The results of these security tests must be included with the annual FTI safeguard report submitted to the CDSS Welfare Fraud Bureau.
- VoIP phones must be logically protected, and CWDs must be able to track and audit all FTI-applicable conversations and access. (If practical, avoid using remote audit/management access and use IP PBX from a physically secure system.)
- Because VoIP technology is compatible with smartphones, but not with many basic mobile phones, and because the IRS' requirements for securing mobile devices and networks are extremely challenging, counties are strictly prohibited from using VoIP mobile phones for FTI.

Because technology changes often, CWDs should monitor the [IRS Office of Safeguards website](#) for updates. This website is located at:

<https://www.irs.gov/privacy-disclosure/safeguards-program>

This website provides information on current and upcoming requirements, resources, and alerts. The current version of [Pub 1075](#) is also available at this site.

Network Protection

Securing networks is highly complex, and CWDs must take precautions to harden and strengthen the boundaries securing FTI. See [Pub 1075](#), Section 9.3.16.5, "Boundary Protection" and Section 9.4.10, "Network Protections."

The CWDs must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems. Counties must not place FTI on publicly accessible servers.

Network address translation (NAT) must be implemented at the public traffic demarcation point on the network. If NAT is not implemented at the CWD boundary firewall or router, then it must be implemented on each firewall or router that protects

network segments that contain infrastructure components which receive, process, store, or transmit FTI.

The CWD's managed interfaces employing boundary protection must deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). All remote traffic must migrate through a managed interface. Firewalls shall be configured to prohibit any transmission control protocol (TCP) or user datagram protocol service or other protocol/service that is not explicitly permitted (i.e., deny by default).

Inbound services shall be prohibited, unless a valid business case can establish their necessity.

In addition, the network boundary must be secured. The information system must:

- a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.
- b. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency networks.
- c. Connect to external networks or information systems only through managed interfaces (see note below) consisting of boundary protection devices arranged in accordance with agency security architecture requirements.

Note: Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

The CWDs must limit the number of external network connections to the information system. The CWDs must:

- a. Implement a secure managed interface for each external telecommunication service.
- b. Establish a traffic flow policy for each managed interface.
- c. Protect the confidentiality and integrity of the information being transmitted across each interface.

All equipment that receives, processes, stores, or transmits FTI must be included as part of an inventory of information systems. This inventory should be updated when any installations, removals, or updates are implemented to the system, or semi-annually at a minimum. See [Pub 1075](#) Section 9.4.12, "System Component Inventory" for more information.

Incoming Calls and VoIP

The technology used by incoming calls falls outside the purview of IRS safeguards and therefore is not covered in this ACL.

Preventing FTI in VoIP

For CWDs with VoIP systems that do not meet the requirements for securing FTI as provided in [Pub 1075](#) and [NIST SP 800-58](#), those CWDs can continue to use landline PSTN phone systems or avoid introducing FTI into their VoIP systems. The following techniques must be used in order to prevent FTI from being input into an unsecure VoIP system.

- Do not provide details from the IRS Asset or BEER matches.
- Do not reveal the source of the information.
- Use vague terms when referencing data and its sources such as “retirement” instead of “your federal retirement benefits from working for the IRS.”
- Let the client provide details. Data sourced from and provided by clients is not FTI. It may be personally identifying information, but it is not FTI.
- Provide the information by fax or by email and follow IRS requirements for securely transmitting FTI by fax or email. (See [Pub 1075](#), Section 9.4.3 “Email Communications” and Section 9.4.4 “Fax Equipment” for more information.)

Do not access or disclose FTI while teleworking, regardless of the means (landline, fax, email, VoIP phone) or any safeguards that protect the transmission of the data. Access to FTI by employees during teleworking is strictly prohibited.

Electronic FTI in VoIP and Contractors

The IRS specifically restricts FTI provided under [IRC 6103\(l\)\(7\)](#) to human services agencies from being disclosed to contractors. The FTI received under this code (IRS Asset and BEER matches) must never be disclosed to contractors. (See [ACL 16-106](#), “[Rediscovery of Federal Tax Information to Contractors](#)” and [Pub 1075](#) Section 5.6 “Human Services Agencies – IRC 6103(l)(7)” for disclosure restrictions and unauthorized disclosure of FTI.) For this reason, the network system components that make up the VoIP system and network used by CWDs must be owned, operated, and administered by the county.

Mobile Devices

Due to the vulnerable nature of wireless connectivity and the challenges associated with securing VoIP networks, the use of mobile VoIP devices (phones or tablets) to access FTI is strictly prohibited. Counties are encouraged to continue to maintain a few “landline” telephones for use with FTI, if possible. If a landline is not available, CWDs may use non-VoIP phones that are not “smartphones.”

These “basic cell phones,” sometimes called “feature phones” because they have one or more features beyond calls, are capable of having these features disabled or deactivated. To be clear, if CWDs choose to use non-VoIP cell phones to discuss FTI, the cell phones must have all features disabled or deactivated with the exception of

calls. Common features that must be disabled or deactivated include, but are not limited to:

- Internet access
- Wi-Fi, Bluetooth, infrared, or any other short-range wireless communications
- Email messaging
- Multi-media messaging service
- Applications such as games, global-positioning, music player, to name a few, installed
- Camera
- Texting

The CWD must own the phones and must have a use policy in place for these cell phones that restricts access to authorized employees.

No Recording

When speaking to a client concerning the FTI from an IRS Asset and/or BEER match, the conversation must not be recorded for any purposes by any person or entity at any time. Recording of conversations that may include FTI is strictly prohibited.

Authorized Employees of the CWD

As a reminder, only CWD employees who meet the following conditions are deemed authorized to access or be able to access FTI:

- Employees of the CWD.
- Have a business need to access FTI to perform their duties or fulfill their responsibilities.
- Passed a background investigation in accordance with [Pub 1075](#) Section 5.1.1 "Background Investigation Minimum Requirements." (A separate ACL on Background Investigations is currently under development.)
- Completed safeguard training specific to FTI.
- Signed a document certifying:
 - Their understanding of their responsibility for safeguarding FTI;
 - Their understanding of the requirement to report incidents or breaches (even suspected) of FTI to the appropriate federal agencies (IRS, Treasury Inspector General for Tax Administration, SSA);
 - Their understanding of the criminal penalties associated with the unauthorized access to and disclosure of FTI.

All County Letter No. 18-37

Page Seven

If you have any questions, please contact the CDSS Welfare Fraud Bureau Safeguard Coordinator at (916) 653-1826, or FraudPrevention@DSS.ca.gov, or your county's IEVS Review Analyst.

Sincerely,

Original Document Signed By:

TODD R. BLAND

Deputy Director

Family Engagement & Empowerment Division