CHILD SUPPORT SERVICES DIVISION
GENERAL PROGRAM ADMINISTRATION
Safeguarding Federal Tax Information & Child Support Information

CS 101.1

SUPERSEDES

Safeguarding Federal Tax and Confidential Child Support Information, July 27, 2023

REFERENCES

18 U.S.C. § 1030; 26 U.S.C. §§ 6103, 7213; 42 USC § 653; 45 CFR 307.13; 45 CFR 303.21; Publication 1075

Applicability

This section is intended to provide guidance for compliance with the Internal Revenue Service's Security Guidelines on safeguarding federal tax information, the Federal Parent Locator Service (FPLS) safeguard and security requirements for receiving FPLS and confidential child support program information. This section is based on Publication 1075 *Tax Information Security Guidelines for Federal, State and Local Agencies* and section H of *Automated Systems for Child Support Enforcement: A guide for States*.

Definitions

Confidential child support program information: Includes state child support program and case information, other state and tribal information, and other confidential information. Confidential information means any information relating to a specific individual or an individual who can be identified by reference to one or more factors including, but not limited to the individual's Social Security Number (SSN), address, employment information and financial information. Any information obtained during the course of a child support investigation that is confidential at its source must be treated as confidential and safeguarded.

Federal Parent Locate Service (FPLS): FPLS information includes information in the National Directory of New Hires (NDNH), the Debtor File and the Federal Case Registry. The NDNH contains new hire, quarterly wage and unemployment insurance information on individuals. The Debtor File contains personal information such as name, SSN, arrearages and other private data. The Federal Case Registry (FCR) contains names, SSNs, state case numbers, dates of birth, sex, abstracts of support orders, and other case information.

Return Information/Federal Tax Information (FTI): According to 26 U.S.C. §§ 6103(2) (A), (B) "return information" also known as FTI is, *(A) a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,*

(B) any part of any written determination or any background file document relating to such written determination (as such terms are defined in section 6110(b)) which is not open to public inspection under section 6110....

Information that is not considered FTI

If the information is provided by the individual or a third party it is not return information. Provided means *actually giving the information,* not just verifying and returning a document that includes return information. Verification received from either the payer (financial, government, or other institution, or employer) or the participant, is **not** FTI if there is no reference, either in writing or verbally, to the fact that the information was originally provided to the CSSD by the IRS. This third-party verification can be used in follow-up casework. If the individual or third party subsequently provides return, return information or personally identifiable information, it is not FTI as long as the IRS source information is replaced with the newly provided information.

Safeguard Review

A Safeguard Review is an evaluation of the use of FTI received from the IRS, the Social Security Administration or other agencies and the measures employed by the receiving agency to protect that data from loss, breach or misuse, and to prevent unauthorized disclosure or access.

Policy

It is the policy of the Child Support Services Division (CSSD) to protect the confidentiality of FTI, FPLS information, and all other confidential child support information, and to comply with the IRS Security Guidelines and other safeguard requirements. As a condition of receiving FTI and participation in the U.S. Department of Treasury offset program, the CSSD is required to meet federal safeguard requirements and to establish and maintain safeguards designed to prevent unauthorized access or disclosure and to maintain the confidentiality of FTI.

The CSSD undergoes an IRS Safeguard Review every three years concerning the security of FTI. Additionally, the CSSD Internal Auditor undertakes an annual inspection and reports the findings to the IRS in the annual Safeguard Security Report. In order to maintain compliance with these reviews the units and regional offices with the CSSD are required to be familiar with IRS standards and expectations for securing FTI and the penalties for unauthorized disclosure.

In addition to FTI, the CSSD receives FPLS information from the federal Office of Child Support Services (OCSS). It is the policy of the CSSD to comply with the security and privacy requirements for receiving FPLS, and confidential CS program information. FPLS and confidential CS information is confidential and must be safeguarded. Access to and disclosure of this information is limited to authorized CSSD staff that needs the information to perform their job duties in accordance with federal laws and regulations. The unauthorized use, misuse or modification of information can result in federal and state civil and criminal penalties, as well as individual disciplinary action.

CSSD Units and Regional Offices

Unit supervisors and regional managers are responsible for ensuring employees receive training for safeguarding FTI, FPLS, and confidential CS program information. In addition, they are responsible for completing the Internal Inspections Report. This requires that they are familiar with the IRS Guidelines for securing FTI and ensuring that all record keeping, physical security, and safeguarding requirements are in place.

It is important that units and regional offices that handle sensitive and confidential information periodically undertake their own review. The following constitutes a minimum inspection for an office handling this type of information:

- A review of the storage and handling of FTI and other confidential information
- An assessment of facility security features.
- A review of after-hours security measures.
- A review of how access to FTI and other confidential information is granted to employees.
- An analysis of security procedures and instructions to employees.
- An annual review of access to safes or filing cabinets or other secure storage containers or areas and of responsibility for changing keys or combinations as well as the exercise of that responsibility. This would include a reconciliation of all key records.
- A review of procedures for, and records of, disposing of or destroying tax information no longer needed by the CSSD.
- Verification that FTI has not been commingled with other information in such a way that its confidentiality could be inadvertently compromised.

Employee Awareness

All employees who are granted access to FTI, FPLS, and CS program information are provided annual disclosure awareness training concerning federal laws and regulations by reviewing the CSSD and Health and Human Services Department policy on safeguarding confidential information and by viewing the IRS educational video. The video provides information on confidentiality, security and penalties for the unauthorized disclosure and destruction of FTI, for the safeguarding of confidential information, and incident response reporting.

Every CSSD employee must annually sign a statement certifying they have received awareness training and understand the policies and procedures for safeguarding FTI, FPLS, and CS program information and the penalties for its unauthorized inspection or disclosure. New employees must receive disclosure awareness training and sign a statement certifying they have received the training **prior** to being granted access to this information. It is the responsibility of the hiring supervisor to notify the SEARCHS Security Team at hhscss007@mt.gov when a new employee has completed the disclosure awareness training. Failure to comply

with the certification requirements may result in loss of access. The certification forms are maintained by the CSSD Central Office.

Equally important to avoid is improper disclosure of FTI, FPLS, and confidential CS program information, which is restricted to CSSD staff with a need-to-know. Do not have conversations that indiscriminately disseminate it.

Paper & Electronic Media FTI

In order to avoid improper inspections, the CSSD does not print reports that contain FTI. Reports containing FTI can be accessed electronically by authorized personnel. System screens containing FTI have been limited and labeled as containing FTI to prohibit unauthorized disclosure. Printed FTI must be clearly labeled as such and logged from the point it is first printed until its destruction. This applies whether it is a report or a screen print from SEARCHS. For example, a print of a payment history screen that contains a federal offset payment. Any printed FTI must be securely stored, safe from unauthorized access. Electronic media containing FTI or converted FTI from paper to electronic media (scanning) also requires logging from the point it is created until its destruction. For example, creating an Excel spreadsheet containing FTI would need to be logged from creation to destruction. Sample log sheets are attached at the end of this section for paper and electronic media containing FTI.

E-mail and Fax

It is forbidden to send FTI via fax or e-mail or e-mail attachment. Use of the Montana File Transfer Service is an alternative to fax and e-mail. If it is necessary to send FTI via the Montana File Transfer Service, extreme caution must be used in the creation and transmission of the file. The following precautions must be taken to protect FTI sent via the Montana File Transfer Service:

- Ensure that all files are sent to the correct address
- The file must be labeled (e.g., contains FTI) to ensure the recipient is aware that the file content contains FTI
- Audit logging must be implemented to properly track all file transfers that contain FTI
- The transmission must be encrypted using FIPS 140-2 validated mechanism, and Malware
- protection must be implemented at one or more points within the file delivery process to
- protect against viruses, worms, and other forms of malware.

If FTI is inadvertently faxed, it is necessary to log where the FTI was sent, who received it, and what actions were taken by the receiver of the faxed FTI (for example: printing, refaxing, storing or destruction). The inadvertently faxed FTI must be treated like paper & electronic media FTI and go through the audit logging process.

Improper Inspections or Disclosures

FTI, FPLS, and confidential CS program information should not be inspected by or disclosed to any person not authorized to receive such information. Examples of avoiding improper inspection of confidential information are ensuring computer monitors are turned to disallow a view of it by a guest, locking screens when you leave your computer, and monitoring the mainframe log-on on information. The mainframe log-on information lists the last time and date an individual accessed the system. Monitoring this information is an effective way to check for improper access to the mainframe under your User ID.

Report Improper Inspection, Disclosure or Misuse

This section covers the actions required for reporting or responding to security incidents involving FTI, FPLS or confidential child support information, including the improper inspection, disclosure or unauthorized use.

All CSSD staff are responsible for reporting known or suspected improper inspection, disclosure or unauthorized use of FTI, FPLS and/or confidential child support information. All incidents must be promptly reported to your immediate supervisor and other authorities as outlined below. Incident response will be handled appropriately based on the type of information involved. All individuals involved in investigating the incident must maintain confidentiality unless the Administrator authorizes information disclosure in advance. An Incident Response Team will oversee the handling and reporting of the incident. The Incident Response Team consists of Program Auditor, Program and Training Bureau Chief, Administrator and the Bureau Chief of the individual reporting.

Upon discovering a possible improper inspection, disclosure or unauthorized use of any confidential information (including child support, FPLS and FTI), including a breach and security incident, immediately notify your supervisor. The supervisor will then immediately contact their Bureau Chief, who will work with the Incident Response Team to directly report the improper inspection and/or disclosure to the appropriate office as instructed below.

FTI information

If FTI is involved, the IRS Program Manager at the IRS Office of Safeguards must be notified. See contact information below. The Office of Safeguards may be able to assist in resolving the situation. Timely notification is the most important factor, but no later than 24 hours after identification.

Procedures

IRS Office of Safeguards email address: SafeguardReports@irs.gov

IRS Office of Safeguards Notification Process

The CSSD must notify the Office of Safeguards. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time of the incident
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)
- Confirm whether CSSD will or may propose an adverse or disciplinary action against an employee for an unauthorized inspection or disclosure of FTI
- Do not include any FTI in the data Incident report
- Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term *data incident report* in the subject line of the email.

Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

The CSSD will cooperate with the Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

The Office of Safeguards will coordinate with the CSSD regarding appropriate follow-up actions required to be taken by the agency to ensure continued protection of FTI. All incidents will be tracked and documented. Once the incident has been addressed, the CSSD will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees immediately.

The CSSD will annually perform a tabletop exercise to test the incident response capability of the agency. This test will analyze various scenarios involving a breach of FTI. Agency staff with incident response duties will be included in the tabletop exercises. After each tabletop exercise a post exercise report must be produced to improve existing policies and procedures.

FPLS and Confidential Child Support Program Information

If FPLS or confidential child support information is involved the FPLS Information Systems Security Officer (ISSO) must be notified. The Administrator or designee must report the incident to the FPLS ISSO designated in the security agreement between the CSSD and the OCSS within one hour of discovery. The Administrator or designee will also notify the FPLS ISSO of any investigation, mitigation and resolution.

Penalties for Unauthorized Inspection of FTI

26 USC § 7213A—Unauthorized inspection of returns or return information, also known as the Taxpayer Browsing Protection Act, states that any unauthorized inspection of Federal returns or return information 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. Additionally, damages for any civil action brought under IRC § 7431 allows for $1,000 for each act of unauthorized inspection or the actual damages sustained, whichever is greater, plus possible punitive damages and the cost of the action. Disclosure restrictions and penalties apply even after employment with the CSSD has ended.

Penalties for Unauthorized Disclosure of FTI

26 USC § 7213, states that willful disclosure of Federal returns or return information is a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution. Additionally, damages for any civil action brought under IRC § 7431 allows for $1,000 for each act of unauthorized disclosure or the actual damages sustained, whichever is greater, plus possible punitive damages and the cost of the action. Disclosure restrictions and penalties apply even after employment with the CSSD has ended.

Employee Disciplinary Action

If the CSSD proposes an adverse or disciplinary action against an employee for an unauthorized inspection or disclosure of FTI a written notification must be sent to the person whose FTI was impacted. The notification must include the date of the unauthorized inspection or disclosure of FTI, and the taxpayer rights listed in IRC § 7431. The CSSD must inform the Office of Safeguards of the written notification prior to notifying the person impacted.

Penalties for unauthorized Access and Use

Unauthorized access, use, or misuse of FPLS, or confidential child support information constitutes a violation of 18 USC 1030 and may subject the individual to disciplinary action, criminal and civil penalties. In addition, pursuant to MCA 15-30-2618 it is unlawful to disclose the amount of income, or any particulars set forth or disclosed in any individual report or return, except as otherwise provided by law. Any offense is punishable by a fine not exceeding $500. An officer or employee of the State must also be dismissed and may not be employed by the State for one year. Confidential information may not be used or disclosed to further a personal interest. A penalty between $50 and $1,000 may be imposed per MCA 2-2-104, 2-2-137.

Commingling of FTI

FTI should be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures. FTI should not be maintained as part of the case files. If physical separation is impractical, the file must be clearly labeled to indicate that federal tax information is included, and the file safeguarded. The FTI information within the file must also be clearly labeled. Labels for this purpose are available from the IRS. Any document containing FTI should be labeled, even if you plan to shred the document. Use a red pen to mark the document as FTI as soon as you retrieve it from the printer.

If FTI is included in an inquiry, verification letter, or in an internal data input form, the FTI NEVER loses its character as return information, even if it is subsequently verified. If the document has both return information and information provided by the individual or a third party, **commingling has occurred,** and the document must be labeled and safeguarded.

If the information is provided by the individual or a third party from their own source, rather than directly from the IRS, the information is not considered return information. **Provided means actually giving the information, not just verifying and returning a document that includes return information**. For example, if a new address is received from IRS records and entered into a computer database, then the address must be identified as FTI and safeguarded. If the address is subsequently provided by the individual or a third party, the information may be reentered and not considered return information.

Confidential Information

FPLS and confidential child support program information received from the OCSS does not lose its character as FPLS or confidential child support program information until its ultimate destruction. This information is confidential and must be safeguarded. Access to and disclosure of this information is limited to authorized CSSD staff that needs the information to perform job duties in accordance with federal law and regulations. Any information obtained during the course of a child support investigation that is confidential at its source must be treated as confidential and safeguarded.

Disposal of Federal Tax Information

Any paper material generated with FTI must be made “undisclosable” in order to protect its confidentiality. After using FTI, precautions must be observed when destroying it. Paper FTI will be destroyed by shredding.

To make reconstruction more difficult:

- The paper must be destroyed using a crosscut shredder that produces particles that are 1mm x 5mm or smaller or pulverize paper materials using disintegrator devices with a 2.4 mm security screen.

If shredding deviates from the above specification, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping. Hand tearing, recycling, or burying information in a landfill **are unacceptable methods of disposal**. More information is available in Section 2.0 of Publication 1075.

Annual Wage Record Data is FTI

Annual Wage Record (AWR) Data is the annual W-2 data submitted by employers. The Social Security Administration manages the data for the IRS. AWR is used for tax purposes and for determination of Social Security benefits. It provides information on all employed individuals reported to the IRS, including self-employed and non-covered employment. Any AWR data is FTI and subject to the FTI safeguard and disclosure requirements.

Other Safeguards

- FTI should not be left lying on your desk.
- If a position requires FTI, FPLS or confidential child support information at an alternate work site, access is only allowed in emergency situations with prior management approval. FTI, FPLS and confidential child support information accessed from an alternate work site remains subject to the same safeguard requirements as outlined in this section.
- It is forbidden to access FTI from a non-state-owned personal computer or mobile device.
- FTI, FPLS and confidential child support information, may not be posted on social media, networking, or other public websites.
- Communication about a federal tax offset (FTO) can only be made with the obligor. Do not discuss FTO payment information with the obligee unless the account must be placed on hold. At that time the obligee can be advised of the hold, but **not the reason for it**. Additionally, the obligee can be informed in general terms about any collection and/or enforcement services that may potentially occur in the case. This includes an FTO because information would not be derived from a federal tax return.

Safeguarding Social Security Numbers

It is important to protect the Social Security Number (SSN) of case participants. A disclosure of someone's SSN could subject that person to identity theft or fraud.

In order to protect case participant's SSNs, the CSSD has implemented a practice to use no SSN or only the last four digits of the SSN on certain documents and reports. Below are other safeguards that will help ensure that the CSSD does not inadvertently disclose a participant's SSN:

- Shred printed documents that contain a participant's SSN.
- Do not include SSNs in fax or e-mail communications unless the same precautions are used as described above for FTI.
- When answering phone calls, don't ask for the SSN as the first form of identity verification. Ask for some other form of identifying information, such as name, case number, participant number, date of birth or address. If none of these are sufficient, it still may be necessary to ask for the SSN.

CHILD SUPPORT SERVICES DIVISION

GENERAL PROGRAM ADMINISTRATION

Safeguarding Federal Tax Information & Child Support Information

CS 101.1

Log of PAPER DOCUMENTS Containing FTI/Print Screens

Name:_____ **Unit:**_____

Name of Document/Screen	Date Printed	# of Pages	Taxpayer Name	Tax Year	Type of Information	Reason	Location of Documents	Who Accessed?	Date of Destruction	Method of Destruction	Comments

CHILD SUPPORT SERVICES DIVISION

GENERAL PROGRAM ADMINISTRATION

Safeguarding Federal Tax Information & Child Support Information

CS 101.1

Log of ELECTRONIC MEDIA FILES Containing FTI

Name:_____ **Unit:**_____

Date Received	File Name	Content	Recipient/ Title-Location	Number of Records	Movement Date	Recipient/ Title-Location	Date of Destruction	Method of Destruction	Comments