IRS AUDIT GUIDE

County	Date
Person Completing: Name	Phone

Pertaining to reports:

S470X615A IRS Match> IRS Data
S470X425A SSA Earnings and Pension Report> IRS Data

Review the storage and handling of federal tax information. See 14-G.

A. Storage of IRS Data

Per Employees' Manual 14-G, these reports are not to be stored in case records. They should be kept in a locked storage area, such as a cabinet or file drawer. The key to the cabinet or file drawer must also be secure. Refer to Section 5.3 of the IRS Publication 1075 on commingling of tax data. Release of information forms 470-3741 and 470-3742 are not considered federal tax information when they are returned by the employers or financial institution and the top portion of the form has been removed. If any other release forms are used, then they are considered IRS data and must be secured in the same manner as the IRS reports.

1. Where are active IRS data stored?

2. Where are closed files kept? Do they contain IRS data?

B. General Security for Handling IRS Data

Per Employees' Manual 14-G, the *IRS Tracking Log* must be kept documenting the receipt of IRS reports. 14-G also specifies that in case of a client move, IRS data should not be forwarded to another county office or institution, unless the data has not been acted upon.

In this situation, the IRS data must be double-sealed in an envelope with the inside envelope marked "Confidential – to be opened by authorized personnel only" before mailing to the new county office or institution. Refer to Section 4.5 of IRS Publication 1075 for federal requirements on office moves and the handling and transporting of federal tax data. **The emphasis is to make sure only employees who *need to know* have access to federal tax data.** See Publication 1075, Section 5.2 for more detail on need to know.

1. Is the *IRS Tracking Log* (470-3563) updated as new IRS reports are received by the county office? (Reviewer must view form.)

2. Is the county office notifying DDM Operations of receipt of IRS data? (See 14-G-Appendix, **IRS Transmittal Process**.)

3. Where are unfiled IRS data reports kept?

4. Who has access to unfiled IRS data?

5. Are interview areas private (to prevent other people hearing discussion of confidential information)?

6. Do employees go to break or lunch and leave their computers available to other persons? Could someone else use an employee's computer to access IEVS data? Do employees use password screen savers or do they log off of the NES screen?

7. Are old case records or files containing IRS data left on a desk or unlocked during working hours? What about after hours?

8. How is federal tax data forwarded to other counties or institutions? First class mail or other method? Are double envelopes used? Is the <u>inside</u> envelope marked confidential?

C. Destruction of IRS Data

Employees' Manual I-C specifies the proper destruction methods to be used for IRS data. Shredding is the most common. Paper strips must be no wider than 5/16" if records are shredded. Hand-tearing or burying the information at a landfill is not acceptable. A DHS employee must perform the destruction or observe the destruction of any IRS data and record the number of reports destroyed and date in the *IRS Tracking Log*. Refer to IRS Publication 1075, page 37, for more information on allowed destruction methods.

1. How are the IRS reports destroyed?

2. If shredding is used, what is the width of the strips?

3. Who destroys the data? (DHS employee or other) (If the destruction is performed by a non-DHS person or a DHS person that does not have a need-to-know, then the destruction must be witnessed by authorized DHS personnel.)

4. Is the log updated when IRS reports are destroyed? (Reviewer must check the *IRS Tracking Log*.)

D. Physical Security

Employees' Manual I-C, **Federal Tax Information**, specifies that care must be taken to deny unauthorized access to areas or files containing federal tax information. This can be accomplished by a variety of methods: signs on doors, locks, security glass, electronic monitoring equipment, card readers, etc. IRS requires a minimum of two barriers for IRS data.

1. Are restricted areas marked? Signs posted? Are there two physical barriers to get to IRS data?

2. Are door hinges to the building and to high security areas on the inside?

3. Are there ground-level windows to the building? If yes, are they made from regular glass? (Security glass should be used. This is defined as a minimum of 2 layers of 1/8" plate glass with .060 (1/32) vinyl interlayer.)

4. Are there other tenants in the building? If yes, are two barriers used to secure federal tax information?

5. What are hours of cleaning crews and building maintenance staff? Are they supervised by a DHS person? Are they left alone to clean? (The <u>two</u> barrier minimum standard is applicable for maintenance staff and landlords. For security and cleaning crews, one barrier is required.)

6. What are usual hours of operation? Who has after-hour access?

7. Is there a record of who enters the building after hours? (If there is no electronic method to record access of individuals, a log would be beneficial to record who entered the building, the time of arrival and departure, and purpose.)

8. Is there after-hour security? Guards? Alarm system? Cameras? Who responds if there is a building break-in?

9. How are building evacuations handled? What about re-entry to the building? (Could unauthorized persons get to IRS data?)

E. Locking Systems for Secured Areas and Security Rooms

Refer to IRS Publication 1075, Section 4.3 (Security of Tax Information), for additional information on keys and locks. Each office or institution should have a list of persons with keys to the office. At a minimum, the list should be reviewed annually to ensure people have not lost their keys or determine if access to the building after hours is still appropriate.

Any key or lock must be "off master." Keys to the building or files containing IRS data should indicate "do not duplicate." Keys to files, cabinets, or rooms containing IRS data should also be secure.

Example: If a person locked the cabinet where IRS reports are stored, then lay the key in a desk drawer for anyone to get it, IRS would consider this a breach in security.) High security pin-tumbler locks are required. Locks are to be double-cylinder design and have 5 or more pin-tumblers.

1. Where are keys for locked desks and cabinets which contain IRS data kept? Who has access to these keys?

2. How is entry into the building controlled during working hours? (Card keys? Elevator codes?) How are unauthorized people prevented from entering areas where IRS data is kept?

3. When an employee terminates, what process is in place to obtain keys to cabinets, desk, etc.? Are access codes changed or locks changed? (<u>This should be done annually.</u>)

4. Are keys marked with “Do not duplicate”?

5. Are keys to files accessible for others to duplicate?

F. Employee Training on Confidentiality

All DHS employees should be familiar with confidentiality requirements and the policy regarding IRS tax data. Employees’ Manual I-C, **Federal Tax Information**, clearly states the consequences if an unauthorized disclosure of IRS data occurs. Also I-C, **Responsibilities of Department Administrators**, lists procedures that should be followed to guarantee confidentiality.

Refer to Publication 1075, Section 6.2, for information on employee awareness. Supervisors should specifically review with staff the IRS policy on confidentiality once a year. Employees’ Manual I-C, **Federal Tax Information**, lists the IRS sections and possible penalties.

1. What training is provided to new workers? How is it documented?

2. Do supervisors routinely review I-C and 14-G with staff? How often?

3. Have all DHS employees signed the annual *Certification* form? Is this documented? Reviewer must include documentation for the annual “Safeguard Report.”

4. Does staff understand the severity and liability issues related to IRS data? Can employees recite the possible penalty provisions?