# Tax Information Security Guidelines for Federal, State and Local Agencies

*Safeguards for Protecting Federal Tax Returns and Return Information*

# TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES

OMB No. 1545-0962

## *Paperwork Reduction Act Notice*

We ask for the information in the Safeguard Procedures Report and the Safeguard Activity Report to carry out the requirements of the Internal Revenue Code (IRC) 6103(p).

You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by Code section 6103.

The information is used by the Internal Revenue Service to assure that agencies, bodies and commissions are maintaining appropriate safeguards to protect the confidentiality of returns and return information. Your response is mandatory.

The time needed to provide this information will vary depending on individual circumstances. The estimated average time is 5 hours.

If you have comments concerning the accuracy of these time estimates or suggestions for making this publication simpler, we would be happy to hear from you. You can write to the Tax Forms Committee, Western Area Distribution Center, Rancho Cordova, CA 95743-0001.

## *Preface*

This publication revises and supersedes Publication 1075 (Rev. 2-96).

# TABLE OF CONTENTS

# TABLE OF CONTENTS



## Exhibits

# INTRODUCTION SECTION 1.0

## *1.1 General*

The self-assessment feature is a distinguishing characteristic and principal strength of American tax administration. The Internal Revenue Service (IRS) is acutely aware that in fostering our system of taxation the public must have and maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection or disclosure. Therefore, we must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of this public trust. The Code makes the confidential relationship between the taxpayer and the IRS quite clear. It also stresses the importance of this relationship by making it a crime to violate this confidence. IRC 7213 prescribes criminal penalties for Federal and State employees and others who make illegal disclosures of Federal tax returns and return information (referred hereafter as Federal tax information). Additionally, IRC 7213A, a recent enactment, makes the unauthorized inspection or disclosure of Federal tax information a misdemeanor punishable by fines, imprisonment or both. Finally, IRC 7431 prescribes civil damages for unauthorized inspection or disclosure and the notification to the taxpayer that an unauthorized inspection or disclosure has occurred. The sanctions of the Code are designed to protect the privacy of taxpayers. Similarly, the IRS recognizes the importance of cooperating to the fullest extent permitted by law with other Federal, State and local authorities in their administration and enforcement of laws. The Service strongly supports the expansion of programs designed to exchange information with State tax agencies. The concerns of citizens and Congress regarding individual rights to privacy make it important that we continuously assess our disclosure practices and the safeguards employed to protect the confidential information entrusted to us. Those agencies or agents that receive Federal tax information directly from the IRS, or receive it from secondary sources (i.e., Health and Human Services, Federal entitlement and lending agencies) must have adequate programs in place to protect the data received.

The Internal Revenue Service is acutely aware that in fostering our system of taxation the public must have and maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection or disclosure.

## *1.2 Overview of the Publication*

This publication is intended to provide guidance in assuring that the policies, practices, controls and safeguards recipient agencies or agents employed adequately protect the confidentiality of the information they receive from the IRS. The guidelines outlined herein apply to all Federal tax information, no matter the media on which it is recorded. Computerized media containing Federal tax information must be afforded the same levels of protection given to paper documents or any other media with Federal tax information. Security policies and procedures, systemic, procedural or manual should minimize circumvention. A mutual interest exists with respect to our responsibility to ensure that Federal tax information is disclosed only to authorized persons and used only as authorized by statute or regulation. The IRS is confident of your diligence in this area and believes that the publication will be helpful. Conformance to these guidelines will meet the safeguard requirements of IRC 6103(p)(4) and make our joint efforts beneficial.

# INTRODUCTION

Security policies and procedures, systemic, procedural or manual should minimize circumvention.

This publication is divided into fourteen sections. Following the Introduction, Sections 2 and 3 address most of the preliminary steps an agency should consider before submitting a request to receive Federal tax information and what to expect from the IRS once the information has been disclosed. Sections 4 through 11 are directed toward the requirements of proper safeguarding and use of Federal tax information as prescribed in the IRC. Sections 12 through 14 address miscellaneous topics that may be helpful in setting up your program. Finally, eight exhibits are provided for additional guidance.

# REQUESTS FOR FEDERAL RETURNS AND RETURN INFORMATION

# SECTION 2.0

## *2.1 General*

Section 6103 of the IRC is a confidentiality statute and generally prohibits the disclosure of Federal tax information. (See Exhibit 1 for general rule and definitions.) However, exceptions to the general prohibition authorize disclosure of Federal tax information to certain Federal, State and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency. Federal tax information so disclosed may be used by the receiving agency solely for the purpose described in the exception authorizing the disclosure. The statutes providing authorization to disclose Federal tax information contain specific conditions that may require different procedures in maintaining and using the information. These conditions are outlined under specific sections in this publication.

As a condition of receiving Federal tax information, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Safeguards must be designed to prevent unauthorized access and uses. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected. An agency must ensure its safeguards will be ready for immediate implementation upon the receipt of the information. Copies of the initial and subsequent requests for data and of any formal agreement must be retained by the agency a minimum of five years as a part of its safeguards recordkeeping system. Agencies should always maintain the latest Safeguard Procedures Report (SPR) on file. The initial request should be followed up by submitting a SPR. It should be submitted to the IRS at least 45 days before the scheduled or requested receipt of Federal tax information. (See Section 9.2 for requirements.)

An agency must ensure its safeguards will be ready for immediate implementation upon the receipt of the informa-

The SPR should include the processing and safeguard procedures for all Federal tax information received and it should distinguish between agency programs and functional organizations using Federal tax information. Multiple organizations or programs using Federal tax information may be consolidated into a single report for that agency. (Agencies requesting Form 8300 information must file separate Safeguard Procedures Reports for this program.) State Welfare and State Child Support Enforcement agencies must file separate reports because they receive data under different Code sections for different purposes.

Note: Agencies should be careful in outlining their safeguard program. Reports that lack clarity or sufficient information will be returned to the submitting agency.

## *2.2 Coordinating Safeguards Within an Agency*

Reports should be submitted to the IRS at least 45 days before the scheduled or requested receipt of Federal tax information.

Because of the diverse purposes for which authorized disclosures may be made to an agency and the division of responsibilities among different, disparate components of an agency, Federal tax information may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of Federal tax return information, the agency should centralize safeguard responsibility and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official assigned these responsibilities should be in a position high enough in the agency's organizational structure to ensure compliance with the agency's safeguard standards and procedures. The selected official should also be responsible for conducting internal inspections, for submitting required safeguard reports to IRS and for any necessary liaison with IRS.

# IRS SAFEGUARD REVIEWS SECTION 3.0

## *3.1 General*

A safeguard review is an on-site evaluation of the use of Federal tax information received from the IRS, the Social Security Administration (SSA) or other agencies and the measures employed by the receiving agency to protect that data. IRS conducts on-site reviews of agency safeguards regularly. Several factors will be considered when determining the need for and the frequency of a review. Generally, reviews of State and local agencies are conducted by IRS District Disclosure personnel. Reviews of Federal agencies and State welfare agencies are conducted by the IRS Office of Governmental Liaison & Disclosure, Office of Safeguards. Child support enforcement agencies receiving Federal tax information under provisions of IRC 6103 (l)(6) and (l)(8) will be reviewed by the IRS liaison District Disclosure office.

## *3.2 Conducting the Review*

A safeguard review is an on-site evaluation of the protection of Federal tax information.

A written review plan will be provided by IRS. The plan will include a list of records to be reviewed (e.g., training manuals, flow charts, awareness program documentation and organizational charts relating to the processing of Federal tax information), the scope and purpose of the review, a list of the specific areas to be reviewed and agency personnel to be interviewed. Reviews cover the six requirements of IRC Section 6103(p)(4). They are Recordkeeping, Secure Storage, Restricting Access, Other Safeguards, Reports, and Disposal. Additionally, Computer Security, and if applicable, IRC 6103(d) Need and Use will be a part of the review. All six requirements along with computer security and need and use are covered in the text of this publication. Observing actual operations is a required step in the review process. Agency employees may be interviewed during the on-site review, generally to clarify procedures or to determine the level of employee awareness of security requirements and IRC penalty provisions. Agency files may be spot checked to determine if they contain Federal tax information. Safeguard reviews are conducted to find out the adequacy of safeguards as opposed to an evaluation of the agency's programs. Upon completion of the review, a report will be issued. The agency will have the opportunity to provide comments that will be included in the report.

## *4.1 General*

Federal, State and local agencies, bodies and commissions, and agents authorized under Section 6103, to receive Federal tax information are required by IRC Section 6103(p)(4)(A) to establish a permanent system of standardized records of requests made by or to them for disclosure of Federal tax information. (See Exhibit 2.) The records are to be maintained for five years.

## *4.2 Electronic Files*

Authorized employees of the recipient agency must be responsible for securing magnetic tapes/cartridges before processing and ensuring that the proper acknowledgment form is signed and returned to the IRS. Inventory records must be maintained for purposes of control and accountability. Tapes containing Federal tax information, any hard copy printout of a tape or any file resulting from the processing of such a tape will be recorded in a log that identifies:

(a) date received

(b) reel /cartridge control number

(c) contents

(d) number of records if available

(e) movement and

(f) if disposed of, the date and method of disposition.

Such a log will permit all tapes (including those used only for backup) containing Federal tax information to be readily identified and controlled. Responsible officials must ensure that the removal of tapes and disks (containing Federal tax information) from the storage area is properly recorded on charge-out records. Semiannual magnetic tape inventories will be conducted. The agency must account for any missing tape by documenting search efforts and notifying the initiator of the loss.

Note: In the event that new information is provided to a state tax agency as a result of matching tapes, the new information is considered federal tax return information and must be afforded the same consideration as other return information received as a result of the match.

Agencies transmitting Federal tax information from a main frame computer to another main frame computer need only account for bulk records transmitted.

## *4.3 Information Other Than That on Magnetic Tape Files*

A listing of all documents received from the IRS must be maintained by:

(a) a taxpayer name

(b) tax year(s)

(c) type of information (i.e., revenue agent reports, Form 1040, work papers, etc.)

(d) the reason for the request

(e) date requested

(f) date received

(g) exact location of the Federal data

(h) who has had access to the data and

(i) if disposed of, the date and method of disposition.

Authorized employees of the recipient agency must be responsible for securing magnetic tapes before processing and ensuring that the proper acknowledgment form is signed and returned to

If the authority to make further disclosures is present, information disclosed outside the agency must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Agencies transmitting Federal tax information from a main frame computer to another main frame computer, as in the case of the SSA sending data to state welfare and child support agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of transmission, the best possible description of the records and the name of the individual making/receiving the transmission.

## *4.4 Recordkeeping of Disclosures to State Auditors*

When disclosures are made by a State tax agency to State Auditors, these requirements pertain only in instances where the Auditors extract Federal tax information for further scrutiny and inclusion in their work papers. In those instances where Auditors read large volumes of records containing Federal tax information, whether in paper or magnetic tape format, the State tax agency need only identify the bulk records examined. This identification will contain the approximate number of taxpayer records, the date of inspection, the best possible description of the records and the name of the individual making the inspection.

## 5.1 General

There are a number of ways that security may be provided for a document, an item, or an area. These include, but are not limited to, locked containers of various types, vaults, locked rooms, locked rooms which have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized and what equipment is available. Proper planning and organization will enhance the security while balancing the costs.

## 5.2 Minimum Protection Standards (MPS)

The Minimum Protection Standards (MPS) system establishes a uniform method of protecting data and items which require safeguarding. This system contains minimum standards which will be applied on a case-by-case basis. Since local factors may require additional security measures, management must analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS has been designed to provide management with a basic framework of minimum security requirements. The objective of these standards is to prevent unauthorized access to Federal tax information.

The objective of the minimum protection standards is to prevent unauthorized access to Federal tax information.

Items and data to be protected are divided into three categories:

Normal Security - information which has not been identified as requiring High Security or Special Protection.

High Security - items which require greater than normal security due to their sensitivity and /or the potential impact of their loss or disclosure.

Special Security - Items which require a specific type of containerization, regardless of the area security provided, due to special access control needs.

The IRS has categorized Federal tax and privacy information as High Security items. The chart below should be used as an aid in determining the method of safeguarding high security items.

**Protection Alternative Chart**

| Protected Item Classification | Perimeter Type | Interior Area Type | Container Type |
|---|---|---|---|
| HIGH SECURITY | | | |
| Alternative #1 | Secured | | Locked |
| Alternative #2 | Locked | Secured | |
| Alternative #3 | Locked | | Security |

## 5.3 Security of Tax Information

Care must be taken to deny unauthorized access to areas containing Federal tax information during duty hours. This can be accomplished by restricted areas, security rooms or locked rooms. In addition, Federal tax information in any form (computer printout, photocopies, tapes, notes, etc.) must be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter; secured area; or containerization.

The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of Federal tax information.

### 5.3.1 Restricted Area

A restricted area is an area to which entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria, security room criteria or provisions must be made to store protectable items in appropriate containers during non-duty hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of Federal tax information.

Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers which control access. The number of entrances should be kept to a minimum. The main entrance should be controlled by locating the desk of a responsible employee at the entrance to assure that only authorized personnel, with an official need, enter. Lesser used entrances should have cameras or electronic intrusion detection devices such as card keys to monitor access.

The restricted area register should be closed out at the end of each month and reviewed by the area supervisor

A restricted area register will be maintained at a designated entrance to the restricted area, and all visitors (persons not assigned to the area) entering the area should be directed to the designated entrance. Visitors entering the area, should enter (in ink) in the register: their name, signature, assigned work area, escort, purpose for entry and time and date of entry.

The entry control monitor should verify the identity of visitors by comparing the name and signature entered in the register, with the name and signature of some type of photo identification card, such as a drivers license. When leaving the area, the entry control monitor or escort should enter the visitor's time of departure.

Each restricted area register should be closed out at the end of each month, and reviewed by the area supervisor/manager. It is recommended that the register be reviewed by a second level of management. Each review should determine the need for access for each individual.

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an Authorized Access List (AAL) can be maintained. Each month a new AAL should be prepared, dated and approved by the restricted area supervisor. Generally individuals on the AAL should not be required to sign in and the monitor should not be required to make an entry in the Restricted Area Register. If there is any doubt as to the identity of the individual prior to permitting entry, the entry control clerk should verify the identity prior to permitting entry.

### *5.3.2 Security Room*

A security room is a room (the primary purpose of which is to store protected items) which has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials -masonry brick, dry wall, etc. - and supplemented by periodic inspection. All doors for entering the room must be locked in accordance with requirements set forth in Section 5.6, "Locking Systems for Secured Areas and Security Rooms," and entrance limited to specifically authorized personnel. Door hinge pins must be nonremovable or installed on the inside of the room.

In addition, any glass in doors or walls will be security glass [a minimum of two layers of 1/8 inch plate glass with .060 inch (1/32) vinyl interlayer. Nominal thickness shall be 5/16 inch.] Plastic glazing material is not acceptable.

Vents or louvers will be protected by an Underwriters' Laboratory (UL) approved electronic intrusion detection system which will annunciate at a protection console, UL approved central station or local police station and given top priority for guard/police response during any alarm situation. Cleaning and maintenance should be performed in the presence of an employee authorized to enter the room.

Secured areas are internal areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours.

### *5.3.3 Secured Area/Secured Perimeter*

Secured areas are internal areas which have been designed to prevent undetected entry by unauthorized persons during non-duty hours. Secured perimeter/secured area must meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods; or any lesser type partition supplemented by UL approved electronic intrusion detection and fire detection systems.
- Unless electronic intrusion detection devices are utilized, all doors entering the space must be locked and strict key or combination control should be exercised.
- In the case of a fence and gate, the fence must have intrusion detection devices or be continually guarded and the gate must be either guarded or locked with intrusion alarms.
- The space must be cleaned during duty hours in the presence of a regularly assigned employee.

### *5.3.4 Containers*

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving or desk and credenza drawers, carts or any other piece of office equipment designed for the storage of files, documents, papers or equipment. Some of these containers are designed for storage only and do not provide protection (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories - locked containers, security containers and safes or vaults.

#### *5.3.4.1 Locked Container*

A lockable container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with lockable drawers. The lock mechanism may be either a built in key or a hasp and lock.

#### *5.3.4.2 Security Container*

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory; combinations will be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files.
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks.
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks.
- Key lock "Mini Safes" properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

Unless electronic intrusion detection devices are utilized, all doors entering the space must be locked and strict key or combination control should be exercised.

#### *5.3.4.3 Safes/Vaults*

A safe is a GSA approved container of Class I, IV, or V ; or an Underwriters laboratories Listings of TRTL-30, TRTL-60, or TXTL-60. A vault is a hardened room with typical construction of reinforced concrete floors, walls and ceilings, utilizes UL approved vault doors and meets GSA specifications.

## *5.4 Locks*

The lock is the most accepted and widely used security device for protecting installations and activities, personnel data, tax data, classified material and government and personal property. All containers, rooms, buildings and facilities containing vulnerable or sensitive items should be locked when not in actual use. However, regardless of their quality or cost, locks should be considered as delay devices only and not complete deterrents. Therefore, the locking system must be planned and used in conjunction with other security measures.

A periodic inspection should be made on all locks to determine each locking mechanism's effectiveness, to detect tampering and to make replacements.

Accountability records will be maintained on keys and will include an inventory of total keys available and issuance of keys.

## *5.5 Control and Safeguarding Keys and Combinations*

Access to a locked area, room or container can only be controlled if the key or combination is controlled. Compromise of a combination or loss of a key negates the security provided by that lock. Combinations to locks should be changed when an employee who knows the combination retires, terminates employment or transfers to another position; or at least once a year. Combinations should be given only to those who have a need to have access to the area, room or container and should never be written on a calendar pad, desk blotters or any other item (even though it is carried on one's person or hidden from view). Combinations (other than safes and vaults), should be maintained by the management. An envelope containing the combination should be secured in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

Keys should be issued only to individuals having a need to access an area, room or container. Accountability records should be maintained on keys and should include an inventory of total keys available and issuance of keys. Periodically a reconciliation should be done on all key records.

The lock is the most accepted and widely used security device for protecting installations and activities, personnel data, tax data, classified material and government and personal property.

## *5.6 Locking Systems for Secured Areas and Security Rooms*

Minimum requirements for locking systems for Secured Areas and Security Rooms are as follows:

High Security pin-tumbler cylinder locks which meet the following requirements:

- Key-operated mortised or rim-mounted dead bolt lock.
- Have a dead bolt throw of one inch or longer.
- Be of double cylinder design. Cylinders are to have five or more pin-tumblers.
- If bolt is visible when locked, it must contain hardened inserts or be made of steel.
- Both the key and the lock must be "Off Master." Convenience type locking devices such as card keys, sequenced button activated locks used in conjunction with electric strikes, etc., are authorized for use only during duty hours.

Keys to secured areas not in the personal custody of an authorized employee and any combinations. will be stored in a security container.

The number of keys or knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals, preferably supervisors, who have a frequent need to access the area after duty hours.

## 5.7 Intrusion Detection Equipment

Intrusion Detection Systems (IDS) are designed to detect attempted breaches of perimeter areas. IDS can be used in conjunction with other measures to provide forced entry protection for after hours security. In addition, alarms for individual and document safety (fire) and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an onsite protection console, a central station or local police station. Intrusion Detection Systems include but are not limited to door and window contacts, magnetic switches, motion detectors, sound detectors, etc., and are designed to set off an alarm at a given location when the sensor is disturbed.

## 5.8 Security During Office Moves

When it is necessary for an office to move to another location, plans must be made to properly protect and account for all Federal tax information. Federal tax information must be in locked cabinets or sealed packing cartons while in transit. Accountability will be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move. IRS material must remain in the custody of an agency employee and accountability must be maintained throughout the move.

When it is necessary for an office to move to another location, plans must be made to properly protect and account for all tax data.

## 5.9 Handling and Transporting Federal Tax Information

### 5.9.1 Handling

The handling of Federal tax information and tax-related documents must be such that the documents do not become misplaced or available to unauthorized personnel. Only those employees who have a need to know and to whom disclosure may be made under the provisions of the statute should be permitted access to Federal tax information.

### 5.9.2 Transporting

Any time Federal tax information is transported from one location to another, care must be taken to provide safeguards. In the event the material is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures. For example, when not in use, and definitely when the individual is out of the room, the material is to be out of view, preferably in a locked briefcase or suitcase.

All shipments of Federal tax information (including magnetic media and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All Federal tax information transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The second envelope should be marked confidential

with some indication that only the designated official or delegate is authorized to open it.

In areas where all of the requirements of a secure area with restricted access cannot be maintained, the data should receive the highest level of protection that is practical.

## *5.10 Physical Security of Computers and Magnetic Media*

Due to the vast amount of data stored and processed by computers and magnetic media, the physical security and control of computers and magnetic media also must be addressed. Whenever possible, computer operations must be in a secure area with restricted access. In situations such as home work sites, remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment should receive the highest level of protection that is practical. Some security requirements must be met, such as keeping Federal tax information locked up when not in use. Tape reels, disks or other magnetic media must be labeled as Federal tax data when they contain such information. Magnetic media should be kept in a secured area under the immediate protection and control of an authorized employee or locked-up. When not in use, they should be promptly returned to a proper storage area/container.

Good security practice requires that inventory records of magnetic media be maintained for purposes of control and accountability. Section 4 "Recordkeeping Requirements," contains additional information on these requirements.

In the event the material is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures.

## *6.1 General*

The increasing use of automated information systems, technology, and related legislation provides for a challenging environment to protect Federal tax information. Automated information systems vary from mainframe computers to microcomputers, including laptops and electronic notebooks. For convenience, "computers," "systems," or "computer systems" will be used interchangeably to represent automated information systems. Telecommunications security requirements are also addressed. Telecommunications is the electronic transfer of data. This transfer may be between networked computers and computers with remote terminals or other data transfers from one location to another. Included in this are electronic transfers of data within the agency (intra) and between the agency and IRS/SSA, (inter) or with any other agency, representative, agent or contractor.

All systems that process Federal tax information must meet the provisions of OMB Circular A-130, Appendix III and Treasury Directive Policy 71-10. Conformance to the guidelines outlined below should meet the requirements of this directive. Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, commonly called the "Orange Book," is used as the basis for the guidelines and may be a source of additional information. Copies may be obtained from: Office of Standards and Products, National Computer Security Center, Fort Meade, MD20755-6000 Attention: Chief, Computer Security Standards.

All automated information systems and networks that process, store, or transmit Federal tax information must meet or exceed the requirements for Controlled Access Protection (C2).

Generally these references state that:

- All computers, that process, store or transmit Federal tax information must meet or exceed Controlled Access Protection (C2) and
- The two acceptable methods of transmitting Federal tax information electronically are encryption and the use of guided media.

## *6.2 Controlled Access Protection - C2*

All computer systems processing, storing and transmitting Federal tax information must have computer access protection controls - (C2). To meet C2 requirements, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance and documentation.

Security Policy - A security policy is a written document describing the system in terms of categories of data processed, users allowed access and access rules between the users and the data. Additionally, it describes procedures to prevent unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system.

Accountability - Computer systems processing Federal tax information must be secured from unauthorized access. All security features must be available (audit trails, identification/authentification) and activated to prevent unauthorized users from indiscriminately accessing Federal tax

information. Everyone who accesses the computer system containing Federal tax information should be accountable. Access controls should be maintained to ensure that unauthorized access does not go undetected. Computer programmers and contractors who have a need to access data bases, and are authorized under the law, should be held accountable for the work performed on the system. The use of passwords and access control measures should be in place to identify who accessed protected information and limit that access to persons with a need to know.

Assurance - The agency must ensure that all access controls and other security features are implemented and are working when it is installed on their computer system. Significant enhancements or other changes to a security system should follow the process of review, independent testing, and installation assurance. The security system must be tested at least annually to assure it is functioning correctly. All anomalies should be corrected immediately.

An independent test should be implemented on the specific computer or computer system to insure that the security system meets the security parameters

Documentation - Design and test documentation must be readily available. The developer or manufacturer should initially explain the security mechanisms, how they are implemented and their adequacy (limitations). This information should be passed on to the security officer or supervisor. Test documentation should describe how and what mechanisms were tested and the results. If recognized organizations/tests/standards are used, then a document to that effect will suffice. For example, a system tested and certified by the National Security Agency (NSA) as meeting certain criteria may have a document stating this fact, without detailed tests/results information. The agency, however, must ensure the documentation covers the exact system and that it includes the specific computer system used by the agency.

Additionally, documentation must include a security features user's guide and a trusted facility manual. The security features user's guide is addressed to the user of the computer system and shall describe the protection mechanisms provided by the security system, guidelines on their use and how they interact. The user's guide may be a part of standard user documentation, such as a chapter, or it may be a separate document, such as its own manual. The trusted facility manual is a manual addressed to the system administrator, such as a System Security Officer, and shall present cautions about security functions and describe privileges that should be controlled when running a secure system. For more information on computer security requirements see Exhibit 7 in the Appendix.

Note: When a security system is designed or purchased for a specific computer or computer system, the security mechanisms must be reviewed to ensure that needed security parameters are met. An independent test should be implemented on the specific computer or computer system to ensure that the security system meets the security parameters. The test may be arranged by the developer but must be done by an independent organization. The NSA has approved some security systems as meeting specified standards. Additional information on these certifications may be obtained by ordering NSA publication "Information Systems Security - Products and Services Catalogue" from the Government Printing Office. Requests for

the catalogue should be addressed to: Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Agencies should assign responsible individuals (Security Officers) with the knowledge of information technology and applications. This individual should be familiar with technical controls used to protect the system from unauthorized entry.

Finally, contingency and backup plans should be in place to ensure the protection of Federal tax information.

## *6.4 Transmitting Federal Tax Information*

The two acceptable methods of transmitting Federal tax information over telecommunications devices are encryption and the use of guided media. Encryption involves the altering of data objects in a way that the objects become unreadable until deciphered. Guided media involves the use of protected microwave transmissions or the use of end to end fiber optics.

Cryptography standards have been adopted by the IRS and can be used to provide guidance for encryption, message authentication codes or digital signatures and digital signatures with associated certification infrastructure. (See Exhibit 8.) The National Institute of Standards and Technology (NIST) announced a Cryptographic Module Validation (CMV) Program on July 17, 1995. This program will validate cryptographic modules for conformance to FIPS 140 -1, Security Requirements for Cryptographic Modules. Agencies may currently purchase implementations containing cryptographic modules tested and validated under the CMV Program. The list can be obtained through the World Wide Web at http://csrc.nist.gov. Cryptographic standards are reviewed every five years.

The two acceptable methods of transmitting Federal tax information over telecommunications devices are encryption and the use of guided media.

Note: At the time of this publication advanced standards were being developed and may be proposed as a replacement standard at the next review in 1998.

Unencrypted cable circuits of copper or fiber optics is an alternative for transmitting Federal tax information. The use of this method is restricted to the geographical boundaries of the continental U.S., Alaska, Hawaii, United States territories and possessions. Adequate measures must be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio transmission. Additional precautions should be taken to protect the cable, i.e., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers.

## 6.4 Remote Access

Accessing data bases containing Federal tax information from a remote location - that is, a location not directly connected to the Local Area Network (LAN) will require adequate safeguards to prevent unauthorized entry. The IRS' policy for allowing access to systems containing tax information is highlighted below.

- Authentification is provided through ID and password; encryption is used over public telephone lines.
- Authentification is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.
- Standard access is provided through a toll - free 1 800 number and through local telephone numbers to local data facilities.
- Both access methods require the purchase of a special modem for every workstation and smart card for every user.

Special modems must be used at each location and every user must have their own smart card when dialing into a system containing tax information.

## 6.5 Internet/Web Sites

Federal, State and local agencies that have Internet capabilities and connections to host servers are cautioned to perform risk analysis on their computer system before subscribing to their use. Connecting the agency's computer system to the Internet will require "firewall" protection to reduce the threat of hackers from accessing data files containing Federal tax information. Firewalls are computers that act as gatekeepers between the agency's main computer and the outside world. At a minimum, they examine the location from which data enter your main system or the location to which data is going, and then choose, based on your instructions, whether to allow transfer of that information. In addition, firewalls monitor the use of your system and keeps a log so you will know if anyone is trying to break in. Other firewalls offer encryption options, which allow you to scramble information into files and make them unreadable.

## 6.6 Electronic Mail

Precautions should be taken to protect Federal tax information sent via E-mail. Messages containing Federal tax information must be attached and encrypted. Do not send Federal tax information in the text of the E-mail. Ensure that all messages sent are to the proper address and that employees log off the computer when away from the area.

## *6.7 Facsimile Machines*

Generally, the telecommunication lines used to send fax transmissions are not secure. However, to reduce the threat of hackers observe the following:

- encrypt the data over a fax communication line.
- place fax machines in a secured area
- contact should be made to the receiving party before sending the transmission.
- check numbers to ensure that the faxed information is not misdirected.

To reduce the threat of hackers, encrypt the data over a fax communication line.

# RESTRICTING ACCESS TO FEDERAL TAX INFORMATION

# SECTION 7.0

## *7.1 General*

Agencies are required by IRC 6103(p)(4)(C) to restrict access to Federal tax information only to persons whose duties or responsibilities require access. (See Exhibit 4.) To assist with this, Federal tax information should be clearly labeled "Federal Tax Information" and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of safeguarding requirements should be used for computer screens.

Agencies must evaluate the need for Federal tax information before the data is requested or disseminated.

## *7.2 A Need to Know*

Good safeguard practice dictates that access to Federal tax information must be strictly on a need-to-know basis. Federal tax information must never be indiscriminately disseminated, even within the recipient agency, body or commission. Agencies must evaluate the need for Federal tax information before the data is requested or disseminated. This evaluation process includes the agency as a whole, down to individual employees and computer systems/data bases.

The potential for improper disclosure is minimized by restricting access to designated personnel. An employee's background and security clearance should be considered when designating authorized personnel. The IRS recognizes that often it is not feasible to limit access to Federal tax information to the individual who receives it; the official may need to forward Federal tax information to technical and clerical employees for necessary processing. However, no person should be given more Federal tax information than is needed in performance of his or her duties. Examples:

In situations where physical separation is impractical, the file should be clearly labeled to indicate that Federal tax information is included.

- When documents are given to a clerk/typist, no Federal tax information should be included unless it is needed in performance of clerical or typing duties.
- When information from a Federal tax return is passed to a technical employee, the employee should be provided only that portion of the return that the employee needs to examine.
- In a data processing environment, individuals may require access to media used to store Federal tax information to do their jobs but do not require access to Federal tax information (e.g., a tape librarian or a computer operator).

## *7.3 Commingling*

To avoid inadvertent disclosures, it is recommended that Federal tax information be kept separate from other information to the maximum extent possible. Agencies should strive to not maintain Federal tax information as part of their case files.

In situations where physical separation is impractical, the file should be clearly labeled to indicate that Federal tax information is included and the file safeguarded. The information itself will also be clearly labeled. Before releasing the file to an individual or agency not authorized access to Federal tax information, care must be taken to remove all such Federal tax information.

If Federal tax information is recorded on magnetic media with other data, it should be protected as if it were entirely Federal tax data. Such commingling of data on tapes should be avoided, if practicable. When data processing equipment is utilized to process or store Federal tax information and the information is mixed with agency data, access must be controlled by:

The Federal tax information never loses its character as return information even if it is subsequently verified or the source becomes coded or unknown.

- Systemic means, including labeling. See Section 6, "Storage - Computer System Security," for additional information.
- Restricting access to the computer to only personnel authorized to see Federal tax information.
- Deguassing all of the data being removed after each use.

Note: Commingled data with multi-purpose facilities results in security risks which must be addressed. If your agency shares physical and/or computer facilities with other agencies, departments or individuals not authorized to have Federal tax information, strict controls, physical and systemic, must be maintained to prevent unauthorized disclosure of this information.

Examples of commingling:

- If Federal tax information is included in an inquiry or verification letter or in an internal data input form, the Federal tax information never loses its character as Federal tax information even if it is subsequently verified. If the document has both Federal tax information and information provided by the individual or third party, commingling has occurred and the document must also be labeled and safeguarded. If the information is provided by the individual or a third party from their own source, this is not return information. "Provided" means actually giving the information on a separate document, not just verifying and returning a document which includes return information.
- If a new address is received from Internal Revenue Service records and entered into a computer data base, then the address must be identified as Federal information 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. Again, "provided" means using the individual's or third party's knowledge or records as the source of the information.

## *7.4 Access to Federal Tax Information via State Tax Files or Through Other Agencies*

Some State disclosure statutes and administrative procedures permit access to State tax files by other agencies, organizations, or employees not involved in tax matters. As a general rule, Section 6103(d) does not permit access to Federal tax return information to such employees, agencies, or other organizations. The Internal Revenue Code clearly provides that Federal tax information will be furnished to State tax agencies only for tax administration purposes and made available only to designated State tax personnel and legal representatives or to the State audit agency for an audit of the tax agency. If you have any questions as to whether particular State employees are entitled to access Federal tax information, your inquiry should be forwarded to the Disclosure Officer at the IRS District Office which serves your location. The IRC does not permit State tax agencies to furnish Federal tax information to other State agencies, tax or non-tax, or to political subdivisions, such as cities or counties, for any purpose, including tax administration. Nor may State tax agencies furnish Federal tax information to any other States, even where agreements have been made, informally or formally, for the reciprocal exchange of state tax information. Also, nongovernment organizations, such as universities or public interest organizations performing research, cannot have access to Federal tax information.

The IRC does not permit State tax agencies to furnish Federal tax information to other State agencies, tax or non-tax, or to political subdivisions, such as cities or counties, for any purpose, including tax administration.

State tax agencies are specifically addressed in the previous paragraph for a number of reasons. However, the situation applies to all agencies authorized to receive Federal tax information. Generally, statutes which authorize disclosure of Federal tax information do not authorize further disclosures. Unless IRC Sec. 6103 provides for further disclosures by the agency, the agency cannot make such disclosures. This applies both within the agency, such as employees or divisions not involved in the specific purpose for which the disclosure is authorized, and outside the agency, including contractors or agencies with which data exchange agreements exist. Agencies may be authorized access to the same Federal tax information for the same purposes, such as State tax agencies, and subdivisions of the same agency may obtain the same type of Federal tax information for different purposes, such as welfare agencies participating in both welfare eligibility verification [IRC Sec. 6103(l)(7)] and child support enforcement [IRC Sec. 6103(l)(6)]. However, in most cases, the disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information. Each agency must have its own exchange agreement with the IRS or with the SSA. When an agency is participating in more than one disclosure authorization, that is, different programs or purposes, each exchange or release of Federal tax information must have a separate agreement or be accomplished directly with IRS or SSA. Unless specifically authorized by the IRC, agencies are not permitted to allow access to Federal tax information to agents, representatives or contractors.

Each agency must have its own exchange agreement with the IRS or with the SSA.

## *7.5 Control Over Processing*

Processing of Federal tax information in magnetic media mode, microfilms, photo impressions, or other formats (including tape reformatting or reproduction or conversion to punch cards or hard copy printout) will be performed pursuant to one of the following three procedures:

Agency Owned and Operated Facility - Processing under this method will take place in a manner which will protect the confidentiality of the information on the magnetic media. All safeguards outlined in this publication must also be followed and will be subject to IRS Safeguard Reviews.

Contractor or Agency-Shared Facility for Tax Administration or Federal Debt Collection - This method may only be used by an agency which processes Federal tax information for tax administration or Federal debt collection purposes. For agencies processing Federal tax information for tax administration purposes, the requirements in Exhibit 5 will be included in a contract in accordance with IRC 6103(n).

The agency must make periodic inspections of the contractor or agency-shared computer facility and keep a written record of such inspections.

The agency must make periodic inspections of the contractor or agency-shared computer facility and keep a written record of such inspections.

Contractor or Agency-Shared Facility for Recipients under the Deficit Reduction Act - Examples of Deficit Reduction Act agencies are those involved with eligibility verification of welfare or other benefit's program or those with respect to whom child support obligations are sought to be established or enforced specified by IRC 6103 (l)(7) and/or the refund offset disclosures authorized by IRC 6103(l)(10). Recipients of return information disclosed by the IRS or by the Social Security Administration under the Deficit Reduction Act are allowed to use a shared facility but only in a manner which does not allow access to Federal tax data to employees of other agencies using the shared facility, or by any other person not entitled to access under provisions of the Act.

Note: The above rules also apply to release of magnetic tape to a private contractor or other agency office if the purpose is merely to erase old tapes for reuse.

## *7.6 Disclosure to Contractors*

Disclosure of Federal tax information is prohibited unless authorized by statute. Agencies having access to Federal tax information are not allowed to use contractors unless authorized by statute. 1099 and W2 information is not authorized by statute to be disclosed to contractors under the (l)(6) and (l)(7) programs.

State and Local Child Support Enforcement IRC 6103(l)(6)- In general, no officer or employee of any state and local child support enforcement agency can make further disclosures of Federal tax information. However, the Welfare Reform Act of 1997 gave authorization to disclose limited information to agents (contractors) of the agency for the purpose of and to the extent necessary in, establishing and collecting child support obligations from, and locating, individuals owing such obligations. The information that may be disclosed to an agent is limited to:

- the address
- social security number(s) of an individual with respect to whom child support obligations are sought to be established or enforced, and
- the amount of the offset against a Federal income tax refund for collection of past due child support.

Federal, State and Local Welfare Agencies IRC 6103(l)(7) - no officer or employee of any federal, state or local agency administering certain programs under the Social Security Act, The Food Stamp Act of 1977, or title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of Federal tax information.

State Tax Officials and State and Local Law Enforcement Agencies IRC 6103(d) - State taxing authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, the administering of State tax laws. However, the IRS, pursuant to Treasury Regulation 301.6103(n) -1, requires that agencies notify the IRS prior to the execution of any agreement to disclose to such a person (contractor), but in no event less than 45 days prior to the disclosure of Federal tax information.

Disclosure of Certain Information to Agencies requesting a Reduction Under Section 6402(c) or 6404(d) IRC 6103 (l)(10) - Agencies receiving Federal tax information under deficit reduction are prohibited from making further disclosures to contractors.

## 8.1 General

IRC Sec. 6103(p)(4)(D) requires that agencies receiving Federal tax information provide other safeguard measures as appropriate to ensure the confidentiality of the Federal tax information.

## 8.2 Employee Awareness

Before granting agency employees access to Federal tax information, employees should be certified that they understand security procedures and instructions requiring their awareness and compliance. As a follow up, employees should be required to maintain their authorization to access data through annual recertification. The initial certification and recertification should be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, employees should be advised of the provisions of IRC Sec. 7213(a), 7213A and 7431. (See Exhibits 3 and 4.) Agencies should make employees aware that disclosure restrictions and the penalties apply even after employment with the agency has ended.

Employees should be advised annually of the civil and criminal penalties for unauthorized inspection or disclosure.

Security information and requirements can be expressed to the appropriate personnel by using a variety of methods, such as:

1. Formal and informal training.
2. Topic of discussion at group and managerial meetings.
3. Install security bulletin boards throughout the work areas.
4. Place security articles in employee newsletters.
5. Route pertinent articles that appear in the technical or popular press to members of the management staff.
6. Display posters with short simple educational messages.

## 8.3 Internal Inspections

Another measure required by the IRS are Internal Inspections by the recipient agency. The purpose is to ensure that adequate safeguards, or security measures, have been maintained. The agency should submit copies of these inspections to the IRS with the annual Safeguard Activity Report. (See Section 9.4 for more information.) To provide an objective assessment, the Inspection should be conducted by a function other than the using function.

To provide reasonable assurance that Federal tax information is adequately safeguarded, the inspection should address the safeguard requirements imposed by the IRC and the IRS. These requirements are discussed in greater detail throughout this publication. Key areas that should be addressed include:

## OTHER SAFEGUARDS

### *I. Recordkeeping*

Each agency, and functions within that agency, should have a system of records that documents requests for, receipt of and disposal of returns or return information (including tapes or cartridges) received directly or indirectly from the IRS or the SSA.

### *II. Secure Storage*

Federal tax information (including tapes or cartridges) must be stored in a secure location, safe from unauthorized access.

### *III. Limited Access*

Access to returns and return information (including tapes or cartridges) must be limited to only those employees or officers who are authorized access by law or regulation and whose official duties require such access.

The physical and systemic barriers to unauthorized access should be reviewed and reported. Included should be an assessment of facility security features.

Agencies should establish a review cycle so that all local offices receiving Federal tax return information are reviewed within a three-year cycle.

### *IV. Disposal*

Upon completion of use, agencies should ensure that the Federal tax information is destroyed or returned to the IRS or the SSA according to the guidelines contained in section 10.

### *V. Computer Security*

The agency's review of the adequacy of their computer security provisions should provide reasonable assurance that:

a)All automated information systems and networks that process, store or transmit Federal tax information meet or exceed the requirements for Controlled Access Protection (C2).

b)Only employees with a need-to-know are permitted access to return information and that systemic safeguards are sufficient to limit unauthorized access and ensure confidentiality.

Agencies should establish a review cycle so that all local offices receiving Federal tax information are reviewed within a three-year cycle. Headquarter office facilities housing Federal tax information and the agency computer facility should be reviewed within an eighteen-month cycle.

Inspection reports, including a record of corrective actions, should be retained by the agency for a minimum of three years from the date the inspection was completed. IRS personnel may review these reports during an on-site Safeguard Review.

A summary of the agency's findings and the corrective actions taken to correct any deficiencies should be included with the annual Safeguard Activity Report submitted to the IRS.

## 9.1 General

IRC 6103(p)(4)(E) requires agencies receiving Federal tax information to file a report that describes the procedures established and utilized by the agency for ensuring the confidentiality of the information received from the IRS. The Safeguard Procedures Report (SPR) is a record of how Federal tax information is processed by the agency; it states how it is protected from unauthorized disclosure by that agency.

After receiving Federal tax information, the agency must file a Safeguard Activity Report (SAR). This report, submitted annually, advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the agency's safeguard procedures; summarizes the agency's current efforts to ensure the confidentiality of the Federal tax information; and finally, certifies that the agency is protecting Federal tax information pursuant to IRC 6103(p)(4) and the agency's own security requirements.

## 9.2 Safeguard Procedures Report

All SPRs must be on an agency's letterhead, signed by the head of the agency or delegate, dated and contain the following information:

### *A. Responsible Officer(s)*

The name, title, address and telephone number of the agency official authorized to request tax information from the IRS.

The name, title, address and telephone number of the agency official responsible for implementation of the safeguard procedures.

### *B. Location of the Data*

The location or functional organization where Federal tax information will be processed or maintained. Include an organization chart or narrative description describing the placement of the using function within the agency. If the information is to be used by more than one functional organization, then the pertinent information must be included for each function.

### *C. Flow of the Data*

A chart or narrative describing the flow of Federal tax information through the agency from its receipt through its return to the Service or its destruction, how it is used or processed and how it is protected along the way. (See specific safeguard requirements below.)

*D. System of Records*

A description of the permanent record(s) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the Federal tax information (including tapes or cartridges). Agencies are expected to be able to provide an "audit trail" for information requested and received, including any copies or distribution beyond the original document/media.

*E. Secure Storage of the Data*

A description of the security measures employed to provide secure storage for the data when it is not in current use. Secure storage encompasses such diverse considerations as locked files or containers, secured facilities, key or combination controls, off-site storage and restricted areas.

*F. Limiting Access to the Data*

A description of the procedures or safeguards employed to ensure access to Federal tax information is limited to those individuals who are authorized access and have a need to know. Describe how the information will be protected from unauthorized access when in use by the authorized recipient(s).

The physical barriers to unauthorized access should be described (including the security features of the facilities where Federal tax information is used or processed) and systemic or procedural barriers.

*G. Disposal*

A description of the method(s) of disposal of the different types of Federal tax information provided by the IRS even if it is not returned to the IRS. The IRS will request a written report that documents the method of destruction and which records were destroyed . (See "D" above.)

*H. Computer Security*

All automated information systems and networks which process, store or transmit sensitive but unclassified information (Federal tax information), must meet or exceed the requirements for Controlled Access Protection (C2) as evaluated by NIST. When transmitting Federal tax information, encryption or guided media must be employed.

1) Microprocessors and Mainframe Systems

Describe the systemic controls employed to ensure compliance with the C2 level of access control.

Additional comments regarding the safeguards employed to ensure the protection of the computer system are also appropriate, including security features of the facility.

2) LANS, WANS, Internet, etc.

Describe in detail the security precautions undertaken if the agency's computer systems are connected or planned to be connected to other systems. Controls must be established according to guidelines from the NIST.

3) Personal Computers / Note Books / Laptops

In the event that Federal tax information is (or is likely to be) used or processed by agency employees on personal computers, the Safeguard Procedures Report must include your procedures for ensuring that all data is safeguarded from unauthorized access or disclosure. Include the procedures to be employed to: ensure secure storage of the disks and the data, limit access to the disk(s) or computer screens and destruction of the data.

*I. Agency Disclosure Awareness Program*

Each agency receiving Federal tax information should have an awareness program under which all employees having access to Federal tax information are notified of the confidentiality provisions of the Internal Revenue Code, a definition of what returns and return information is and the civil and criminal sanctions for unauthorized inspection or disclosure. A description of the formal program should be included in the SPR.

## *9.3 Submission of Safeguard Procedures Report*

Federal agencies and State welfare agencies requesting Federal tax information should submit their report to:

National Director
Governmental Liaison and Disclosure CP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224

State taxing agencies and child support enforcement agencies should submit their report to the Liaison District Director's Office of the Internal Revenue Service for your state.

## *9.4 Annual Safeguard Activity Report*

All SARs must be on an agency's letterhead, signed by the head of the agency or delegate, and contain the following information:

*A. Changes to Information or Procedures Previously Reported*

1) Responsible Officers or Employees

2) Functional Organizations Using the Data

3) Computer Facilities or Equipment and System Security - Changes or Enhancements

4) Physical Security - Changes or Enhancements

5) Retention or Disposal Policy or Methods

### *B. Current Annual Period Safeguard Activities*

1) Agency Disclosure Awareness Program

Describe the efforts to inform all employees having access to Federal tax information of the confidentiality requirements of the IRC, the agency's security requirements and the sanctions imposed for unauthorized inspection or disclosure of return information.

2) Reports of Internal Inspections

Copies of the Inspection Reports and a narrative of the corrective actions taken (or planned) to correct any deficiencies, should be included with the annual SAR.

3) Disposal of Federal Tax Information

Report the disposal of Federal tax information or the return to the IRS or source. The information should be adequate to identify the material destroyed and the date and manner of destruction.

### *C. Actions on Safeguard Review Recommendations*

The agency should report all actions taken, or being initiated, regarding agreed-upon recommendations of a safeguard review.

### *D. Planned Actions Affecting Safeguard Procedures*

Any planned agency action that would create a major change to current procedures or safeguard considerations should be reported. Such major changes would include, but are not limited to, new computer equipment, facilities or systems, or use of contractors (as permitted by law or regulation) to do programming, processing or administrative services requiring access to Federal tax information.

## *9.5 Filing Deadlines for the Safeguard Activity Report*

### *A. Federal Agencies*

Reports should be submitted for the calendar year by January 31 of the following year to:

National Director
Governmental Liaison and Disclosure CP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224

*B. State Tax Agencies*

State tax agencies should submit their SARs for the calendar year by January 31 of the following year to the District Director, (Attention: Disclosure Officer) of the IRS district having liaison responsibility.

*C. State Child Support Enforcement Agencies*

State child support enforcement agencies should submit their SARs for the calendar year by January 31 of the following year to the District Director, (Attention: Disclosure Officer) of the IRS district having liaison responsibility.

*D. State Welfare Agencies/DC Retirement Board*

State welfare agencies should submit their reports for the processing year (July 1 through June 30) by September 30 to:

National Director
Governmental Liaison and Disclosure, CP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224

*E. Law Enforcement Agencies Receiving 8300 Information*

Federal, State and local law enforcement agencies should submit their reports for the processing year (July 1 through June 30) by September 30 to:

National Director
Governmental Liaison and Disclosure, CP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224

# DISPOSAL OF TAX INFORMATION UPON COMPLETION OF USE

# SECTION 10.0

## *10.1 General*

Users of Federal tax information are required by IRC 6103(p)(4)(F) to take certain actions upon completion of use of the information in order to protect its confidentiality (See Exhibit 4).

## *10.2 Destruction Methods*

Agency officials and employees will either return the information (including any copies made) to the office from which it was originally obtained or make the information undisclosable and include in the agency's annual report a description of the procedures used. In those cases where the agency elects to return the information, a receipt process must be used (see Section 5.9.2, "Transporting").

The following precautions should be observed when Federal tax information is destroyed:

- Material furnished to the user and user generated material such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes and work papers should be destroyed by burning, mulching, pulping, shredding, or disintegrating.
- Burning precautions: The material is to be burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle should be separated to ensure that all pages are consumed.
- Shredding precautions: To make reconstruction more difficult, the paper should be inserted so that lines of print are perpendicular to the cutting line; small amounts of shredded paper should not be allowed to accumulate in the shredder bin. The paper should be shredded to effect 5/16-inch wide or
- smaller strips; microfilm should be shredded to effect a 1/35-inch by 3/8-inch strips.
- Pulping should be accomplished so that all material is reduced to particles one inch or smaller.
- Destruction of the data should be witnessed by an agency employee to safeguard the data from unauthorized disclosure.

Agency officials and employees will either return the information (including any copies made) to the office from which it was originally obtained or make the information undisclosable.

## *10.3 Other Precautions*

Federal tax data must never be disclosed to contractors unless authorized or to unauthorized agents during disposal. Destruction of the data should be witnessed by an agency employee to safeguard the data from unauthorized disclosure. The Department of Justice, State tax agencies, and the Social Security Administration may be exempted from the requirement of having

agency personnel present during destruction by a contractor, if the contract includes the safeguard provisions required by the Code of Federal Regulations (CFR) 301.6103(n)-1. The required safeguard language is contained in Exhibit 6.

After it has served its purpose, magnetic tape containing Federal tax data must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape should be destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration.

Whenever disk media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any Federal tax information on it must be destroyed by:

- Completely overwriting all data tracks a minimum of three times, using maximum current that will not damage or impair the recording equipment; or
- Running a magnetic strip, of sufficient length to reach all areas of the disk over and under each surface a minimum of three times. If the information cannot be destroyed as suggested, the disk will be damaged in an obvious manner to prevent use in any disk drive unit and discarded.

Note: Hand tearing or burying information in a land fill are unacceptable methods of disposal.

## *11.1 General*

Any agency which receives Federal tax information for an authorized use under IRC Section 6103(d)(1) may not use Federal tax information in any manner or for any purpose not consistent with that authorized use. If an agency needs Federal tax information for a different authorized use under a different provision of lRC 6103, a separate request under that provision is necessary. An unauthorized secondary use is specifically prohibited and may result in discontinuation of disclosures to the agency and in the imposition of civil or criminal penalties on the responsible officials.

## *11.2 State Tax Agencies*

Federal tax information may be obtained by State tax agencies only to the extent the information is needed for, and is reasonably expected to be used for, State tax administration. An agency's records of the Federal tax information it requests should include some account of the result of its use (e.g., disposition of closed cases and summary of revenues generated) or why the information was not used. If an agency receiving Federal tax information on a continuing basis finds it is receiving information which, for any reason, it is unable to utilize, it should contact the IRS official responsible for liaison with respect to the continuing disclosure and modify the request. In any case, IRS will disclose Federal tax information only to the extent that a State taxing agency satisfactorily establishes that the requested information can reasonably be expected to be used for an authorized purpose.

NOTE: IRS conducts annual on site evaluations of "need and use."

IRS will disclose Federal tax information only to the extent that the State taxing agency satisfactorily establishes that the requested information can reasonably be expected to be used for an authorized purpose.

# USE OF RETURN INFORMATION IN STATISTICAL REPORTS

# SECTION 12.0

## *12.1 General*

Section 6103 of the Code authorizes the disclosure of Federal tax information for use in statistical reports used for tax administration purposes and certain other purposes specified in lRC 6103(j). However, such statistical reports may only be released in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

Agencies authorized to produce statistical reports must adhere to the following guidelines or an equivalent alternative which has been approved by the IRS:

- Access to Federal tax information must be restricted to authorized personnel;
- No statistical tabulation may be released with cells containing data from fewer than three returns;
- Statistical tabulations prepared for geographic areas below the State level may not be released with cells containing data from fewer than ten returns, and
- Tabulations which would pertain to specifically identified taxpayers or which would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

Agencies and organizations seeking statistical information from IRS should make their requests under IRC Section 6108(b). The requests should be addressed to: Director, Statistics of Income Division; CP:S Internal Revenue Service, 1111 Constitution Avenue, NW. Wash., DC 20224.

Statistical reports may only be released in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

# REPORTING IMPROPER INSPECTIONS OR DISCLOSURES

# SECTION 13.0

## *13.1 General*

Upon discovery of a possible improper inspection or disclosure of Federal tax information by a Federal employee, a State employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate Internal Revenue Service Regional lnspector.

| REGIONAL INSPECTION OFFICE | REGION | STATES SERVED BY REGION | TELEPHONE NUMBER |
|---|---|---|---|
| Los Angeles, CA | Western | Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, Wyoming | (510) 210-7000 |
| Dallas, TX | Midstates | Arkansas, Iowa, Illinois, Kansas, Missouri, Minnesota, Nebraska, North Dakota, Oklahoma, South Dakota, Wisconsin, Texas | (972) 308-1371 |
| New York, NY | Northeast | Connecticut, Maine, Massachusetts, Michigan, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont | (212) 466-4700 |
| Chamblis, GA | Southeast | Alabama, Delaware, District of Columbia, Florida, Georgia, Indiana, Kentucky, Louisiana, Maryland, Mississippi, North Carolina, South Carolina, Tennessee, Virginia, West Virginia | (770) 986-6900 |
| New York, NY | International | Commonwealth of Puerto Rico, Virgin Islands, Guam, American Samoa, Commonwealth of North Mariana Islands, & Trust Territory of the Pacific Islands | (212) 466-4700 |

## *14.1 General*

If the confidentiality of Federal tax information can be adequately protected, alternative work sites, such as employees' homes or other non-traditional work sites can be used. Despite location, Federal tax information remains subject to the same safeguard requirements and the highest level of attainable security. The following guidelines set forth minimum standards that must be established and maintained. Although the guidelines are written for employees' homes, the requirements apply to all alternative work sites.

## *14.2 Equipment*

Only agency-owned computers and software will be used to process, access, and store Federal tax information. The agency must retain ownership and control of all hardware, software, telecommunication equipment and data placed in the homes of employees.

Employees should have a specific room or area in a room that has the appropriate space and facilities for the type of work done. Employees should also have a means to facilitate communication with their managers or other members of the agency in case security problems arise.

The agency should give employees locking file cabinets or desk drawers so that documents, disks, tax returns, etc. may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the work site.

The agency should provide "locking hardware" to secure ADP equipment to large objects such as desks or tables. Smaller, agency-owned equipment should be locked in a filing cabinet or desk drawer when not in use.

## *14.3 Transmission and Storage of Data*

Federal tax information may be stored on hard disks only if agency-approved security access control hardware/software has been installed and is being used. Access control should include password security, an audit trail, encryption or guided media (see Section 7.4 Transmitting Federal tax Information), virus detection and data overwriting capabilities.

Access control should include password security, an audit trail, encryption or guided media, virus detection and data overwriting capabilities.

## *14.4 Other Safeguards*

The agency should provide specialized training in security, disclosure awareness, and ethics for all participating employees and man-

Only agency-approved security access devices and agency-approved software will be used. Copies of illegal and non-approved software will not be used. Magnetic media that are to be reused must have files overwritten or degaussed.

A plan for the security of alternative work site computer systems will be prepared by the implementing agency. The agency should coordinate with the management of host system(s) and any networks. Before implementation, the agency will perform tests and certify that the security controls are adequate for security needs. Additionally, the agency will promulgate rules or procedures to ensure that computers are not left unprotected any time by the employee. These rules should address brief absences away from the computer.

The agency should provide specialized training in security, disclosure awareness and ethics for all participating employees and managers. This training should cover situations that could occur as the result of an interruption of work by family, friends or other sources.

Periodic inspections of alternative work sites should be conducted by the agency during the year to ensure that safeguards are adequate. The results of each inspection should be fully documented. IRS reserves the right to visit alternative work sites while conducting safeguard reviews.

Changes in safeguard procedures should be described in detail by the agency in their Safeguard Activity Report, or, if applicable, Safeguard Procedures Report. (See Section 9, Reporting Requirements, for details.)

# EXHIBIT 1

## *IRC SEC. 6103. CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION.*

(a) GENERAL RULE.—Returns and return information shall be confidential, and except as authorized by this title—

(1) no officer or employee of the United States,

(2) no officer or employee of any State, any local child support enforcement agency, or any local agency administering a program listed in subsection (l)(7)(D) who has or had access to returns or return information under this section, and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (6) or (12) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n),

shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes on this subsection, the term "officer or employee" includes a former officer or employee.

(b) DEFINITIONS.—For purposes of this section—

(1) RETURN.—The term "return" means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereof, including supporting schedules, attachments, or lists which are supplemental to, or part of the return filed.

(2) RETURN INFORMATION.—The term "return information" means—

(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, over assessments, 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, and

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 the public inspection under 6110,

but such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of the law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

(3) TAXPAYER RETURN INFORMATION.—The term "taxpayer return information" means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.

(4) TAX ADMINISTRATION.—The term "tax administration" —

(A) means—

(i) the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws and related statutes (or equivalent laws and statutes of a State) and tax convention to which the United States in a party, and

(ii) the development and formulation of Federal tax policy relating to existing or proposed internal revenue laws, related statutes and tax conventions and

(B) includes assessments, collection, enforcement, litigation, publication and statistical gathering functions under such laws, statutes, or conventions.

(5) STATE.—The term "state" means—

(A) any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, the Canal Zone, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, and

(B) for purposes of subsection (a)(2), (b)(4), (d)(1), (h)(4) and (p) any municipality—

(i) with a population in excess of 250,000 ( as determined under the most recent decennial United States census data available),

(ii) which imposes a tax on income or wages, and

(iii) with which the Secretary (in his sole discretion ) has entered into an agreement regarding disclosure.

(6) TAXPAYER IDENTITY.—The term "taxpayer identity" means the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in section 6109), or a combination thereof.

(7) INSPECTION.—The terms "inspected" and "inspection" mean any examination of a return or return information.

(8) DISCLOSURE.—The term "disclosure" means the making known to any person in any manner whatever a return or return information.

(9) FEDERAL AGENCY.—The term "Federal agency" means an agency within the meaning of section 551(1) of title 5, United States Code.

(10) CHIEF EXECUTIVE OFFICER.—The term "chief executive officer" means, with respect to any municipality, any elected official and the chief official (even if not elected) of such municipality.

# EXHIBIT 2

## *SEC.6103(p)(4) SAFEGUARDS*

(4) SAFEGUARDS.—Any Federal agency described in subsection (h)(2), (h)(6), (i)(1), (2), (3), (5), or (8), (j)(1) or (2), (l) (1), (2), (3), (5), (11), (13) or (14), (15), or (o)(1), the General Accounting Office, or any agency, body or commission described in subsection (d), (i)(3)(B)(i) or (8) of (l)(6), (7), (8), (9), (10), or (12) or shall, as a condition for receiving returns or return information-

(A) establish and maintain, to the satisfaction of the Secretary, a permanent system of standardized records with respect to any request, the reason for such request, and the date of such request made by or of it and any disclosure of return or return information made by or to it;

(B) establish and maintain, to the satisfaction of the Secretary, a secure area or place in which such returns or return information shall be stored;

(C) restrict, the satisfaction of the Secretary, access to the returns or return information only to persons whose duties or responsibilities require access and to whom disclosure may be made under the provisions of this title;

(D) provide such other safeguards which the Secretary determines (and which he prescribes in regulations) to be necessary or appropriate to protect the confidentiality of the returns and return information;

(E) furnish a report to the Secretary, at such time and containing such information as the Secretary may prescribe, which describes the procedures established and utilized by such agency, body, or commission or the General Accounting Office for ensuring the confidentiality of returns and return information required by this paragraph; and

(F) upon completion of use of such returns or return information-

(i) in the case of an agency, body or commission described in subsection (d), (i)(3)(B), or (l)(6), (7), (8), or (9) return to the Secretary such returns or return information (along with any copies made therefrom) or make such returns or return information undisclosable in any manner and furnish a written report to the Secretary describing such manner

(ii) in the case of an agency described in subsection (h)(2), (h)(6), (i)(1), (2), (3), (5), or (8), (j)(1) or (2), (l)(1), (2), (3), (5), (10), (11), (12), (13) or (14), (15), or (o)(1), or the General Accounting Office, either-

(I) return to the Secretary such returns or return information (along with any copies made therefrom)

(ll) otherwise make such returns or return information undisclosable, or

(lll) to the extent not so returned or made undisclosable, ensure that the conditions of subparagraphs (A), (B), (C), (D), and (E) of this paragraph continue to be met with respect to such returns or return information, and

(iii) in the case of the Department of Health and Human Services for purposes of subsection (m)(6), destroy all such return information upon completion of its use in providing the notification for which the information was obtained, so as to make such information undisclosable;

except that conditions of subparagraph (A), (B), (C), (D), and (E) shall cease to apply with respect to any return or return information if, and to the extent that, such return or return information is disclosed in the course of any judicial or administrative proceedings and made a part of the public record thereof. If the Secretary determines that any such agency, body, or commission or the General Accounting Office has failed to, or does not, meet requirements of this paragraph, he may, after any proceedings for review establish under paragraph (7), take such actions as are necessary to ensure such requirements are met, including refusing to disclose returns, or return information to such agency, body, or commission or the General Accounting Office until he determines that such requirements have been or will be met. In the case of any agency which receives any mailing address under paragraph (2), (4), (6) or (7) of subsection (m) and which discloses any such mailing address to any agent,

or which receives any information under paragraph (6)(A) or 12(B) of subsection (l) and which discloses any such information to any agent this paragraph shall apply to such agency and each such agent (except that, in the case of an agent, any report to the Secretary or other action with respect to the Secretary shall be made or taken through such agency). For purposes of applying this paragraph in any case to which subsection (m)(6) applies, the term "return information" includes related blood donor records (as defined in section 1141(h)(2) of the Social Security Act).

# EXHIBIT 3

## *IRC SEC. 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION.*

(a) RETURNS AND RETURN INFORMATION.—

(1) FEDERAL EMPLOYEES AND OTHER PERSONS.—It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be 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, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES.—It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6130(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (l)(6), (7), (8), (9), (10), (12), or (15) or (m)(2), (4), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS.—It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in an manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION.—It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS.—-It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

## *SEC.7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION*

(a) PROHIBITIONS.—

(1) FEDERAL EMPLOYEES AND OTHER PERSONS.—It shall be unlawful for—

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES.—It shall be unlawful for any person [not described in paragraph(1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY.—

(1) IN GENERAL.—Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES.—An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS.—For purposes of this section, the terms “inspect”, “return”, and “return information” have respective meanings given such terms by section 6103(b).

# EXHIBIT 4

## *IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION.*

(a) IN GENERAL.—

(1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES.—If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF UNITED STATES.—If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) EXCEPTIONS.—No liability shall arise under this section with respect to any inspection or disclosure —

(1) which results from good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) DAMAGES.—In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of—

(1) the greater of—

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of—

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) PERIOD FOR BRINGING ACTION.—Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) NOTIFICATION OF UNLAWFUL INSPECTION AND DISCLOSURE.—If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of—

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or

(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) DEFINITIONS.—For purposes of this section, the terms "inspect", "inspection","return" and "return information" have the respective meanings given such terms by section 6103(b).

(g) EXTENSION TO INFORMATION OBTAINED UNDER SECTION 3406.—For purposes of this section—

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

# EXHIBIT 5

## *CONTRACT LANGUAGE FOR AUTOMATED DATA PROCESSING SERVICES*

The following clauses are required in all contracts for automated data processing services:

I. In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) No work involving information furnished under this contract will be subcontracted without the specific approval of the IRS.

(7) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, the IRS reviewing office.

(8) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(9) (Include any additional safeguards that may be appropriate.)

II. Criminal/Civil Sanctions:

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n).

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

III. Inspection:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

# EXHIBIT 6

## *CONTRACT LANGUAGE FOR DESTRUCTION SERVICES*

The following clauses are required in all contracts for destruction services:

I. PERFORMANCE:

In performance of this contract, the contractor agrees to comply and assume responsibility for compliance by his/her employees with the following requirements:

(1) All work shall be performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any return or return information made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Disclosure to anyone other than an officer or employee of the contractor shall be prohibited.

(3) (Include here any additional safeguards that may be appropriate). See Section 10, "Disposal of Tax Information Upon Completion of Use."

II. Criminal/Civil Sanctions:

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n).

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited, willfully

discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

III. Inspections:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

# EXHIBIT 7

## *COMPUTER SECURITY REQUIREMENTS*

### *Trusted Computer Base (TCB)*

The totality of protection mechanisms within a computer system — including hardware, firmware, and software — the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administration personnel of parameters (e.g., a user's clearance) related to the security policy.

### *SECURITY POLICY*

(1) OBJECT REUSE.—A means of preventing unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system. If an object, such as a disk, tape or storage devices which may be used for printing, file servers, etc., is to be taken out of a system and made available for other uses, it must be cleared of all protected information. This does not include tapes/disks which are used to store data for reuse in the same program or tapes/disks which are specifically assigned to a single program and to which only individuals with the same authorizations and need-to-know have access to the data. Objects being allocated into the system also must not contain residual protected data which other users may access.

(2) DISCRETIONARY ACCESS CONTROL (DAC).—A means of restricting access to objects based on the identity and need-to-know of the users and/or groups to which they belong. All computer systems with Federal tax information must have, as a minimum, discretionary access control.

### *ACCOUNTABILITY*

(1) IDENTIFICATION\AUTHENTIFICATION.—Ensure individual accountability through identification and authentication of each individual system user. Identification and authentication is often accomplished with user ID's and passwords. Passwords must be constructed, protected, and administered in accordance with current Federal standards. The current standard is Federal Information Processing Standards Publication (FIPS PUB) 112, "Password Usage." FIPS publications are sold by the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA. 22161. The system may use any method which uniquely identifies users and requires proof of identity before accessing the system. Identification/authentication must be an auditable function.

(2) AUDIT.— Maintain an audit trail of accesses to the objects and data it protects. The audit trail is a systemic record that is sufficient to enable reconstruction and/or review of activities related to operations, procedures, or events occurring on that system. Audit trails must, at a minimum, be able to record log-in attempts, password changes, and file creations, changes and/or deletions. The audit trail must be protected in such a way that it can not be changed by the user. Audit trails must be reviewed regularly by supervisory, security, or other authorized agency individuals who are not the regular program users. If contractors are authorized, they may be allowed to audit the system. However, the agency must have some review and control procedure to ensure audit trails are being examined regularly. Anomalies must be reported to appropriate supervisory and/or security personnel for follow-up action.

*ASSURANCE*

(1) SYSTEM ARCHITECTURE.—The Trusted Computer Base (TCB) shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

(2) SYSTEM INTEGRITY.—Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

(3) SECURITY TESTING.—The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be found to assure that there are no obvious ways for an unauthorized user to bypass or other wise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

*DOCUMENTATION*

(1) SECURITY FEATURES USER'S GUIDE.—A single summary, chapter, or manuel in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) TRUSTED FACILITY MANUEL.— A manuel addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

(3) TEST DOCUMENTATION.—The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security, mechanism's functional testing.

(4) DESIGN DOCUMENTATION.— Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

# EXHIBIT 8

## *ENCRYPTIONS STANDARDS*

A. Federal Security Standards

The Digital Encryption Standard (FIPS 46 - 2)
Computer Data Authentication (FIPS 113)
Security Requirements for Cryptographic Mod. (FIPS 140 -1)
Key Management using ANSI X9.17 (FIPS 171)
The Digital Hash Standard (FIPS 180 -1)
Escrowed Encryption Standard (FIPS 185)
The Digital Signature Standard (FIPS 186)
Public Key Cryptographic Entity Authentification Mechanism (FIPS 196)

B. Industry Security Standards

Digital Certificate (ANSI X5.09)
Public Key Cryptographic Using Irreversible Algorithms (ANSI X9.30)
Symmetric Algorithm Keys Using Diffie - Hellman (ANSI X9.42)
Extension to Public Key Certificates and Certificate Renovation List (ANSI X9.55)
Message Confidentiality (ANSI X9.23)
Message Authentication Codes (ANSI X9.9)
Management Controls (ANSI X9.45)
Financial Institution Key Management (ANSI X9.17)

## *KEY MANAGEMENT STANDARDS*

FIPS 171 Key Management using ANSI X9.17,

Financial Institution Key Management (ANSI X9.17),

FIPS publications are sold by the National Technical Information Services, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA. 22161.

Department of the Treasury
**Internal Revenue Service**
Publication 1075 (Rev. 1-98)
Catalog Number 469370