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 IRC 6103.

The information is used by the Internal Revenue Service (IRS) to ensure 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 40 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. 3-99).

HIGHLIGHTS FOR 2000

COMPUTER SECURITY

The new international computer security standard for securing sensitive information is International Standards Organization (ISO) 15408 called the "Common Criteria". This security standard, which includes both a description of the security functionality (Protection Profile) and the level of assurance (EAL) associated with an organization's security needs or a product's capability supercedes the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) C2 class. All agencies that receive, process, store, or transmit Federal tax information are required to adhere to the Common Criteria's latest version (currently 2.1). Agency initiatives started prior to October 1, 1999 to comply with C2 requirements are given a temporary waiver. However, by the end of 2001, all products which were previously evaluated against the C2 rating shall be migrated to the Common Criteria evaluation rating.

INTERNET ACCESS

Agencies can access Publication 1075 on the Internet. Go to

ftp://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf

SECURE TRANSMISSIONS

IRS policy for Fax transmissions has been revised. See Section 5.9, page 23 for details.

MAILING REPORTS

All reports (i.e., Safeguard Activity Report, Safeguard Procedures Report, Agency Response to Safeguard Review Report) can be transmitted electronically. Please refrain from sending any tax information in the report. The E-mail address is:

SafeguardReports@irs.gov

SAFEGUARD REVIEWS

As a result of the Restructuring Reform Act of 1998, all Safeguard Reviews will be conducted by the Office of Communications and Liaison, Office of Governmental Liaison and Disclosure.

REPORTING UNAUTHORIZED DISCLOSURES

Unauthorized inspection or disclosure of Federal tax information should be reported to the appropriate Agent-in-Charge, Treasury Inspector General.

Mailing Address:

Treasury Inspector General for Tax Administration
Ben Franklin Station P.O. Box 589
Washington, DC 20044-0589

Hotline Number:
1-800-366-4484

TABLE OF CONTENTS

Section	Title	Page
1.0	**Introduction**	1
1.1	General	1
1.2	Overview of Publication 1075	1
2.0	**Requesting Federal Tax Information and Reviews**	3
2.1	General	3
2.2	Need and Use - IRC 6103(d)	3
2.3	Coordinating Safeguards Within an Agency	4
2.4	State Tax Agencies	4
2.5	IRS Safeguard Reviews IRC 6103(p)(4)	4
2.6	Safeguard Review Report	4
3.0	**Record Keeping Requirements - IRC 6103(p)(4)(A)**	7
3.1	General	7
3.2	Electronic Files	7
3.3	Information Other Than That In Electronic Form	7
3.4	Record Keeping of Disclosures to State Auditors	8
4.0	**Secure Storage - IRC 6103(p)(4)(B)**	9
4.1	General	9
4.2	Minimum Protection Standards	9
4.3	Security of Tax Information	9
4.4	Security During Office Moves	12
4.5	Handling and Transporting Federal Tax Information	13
4.6	Physical Security of Computers and Magnetic Media	13
4.7	Alternate Work Sites	13
5.0	**Restricting Access - IRC 6103(p)(4)(C)**	17
5.1	General	17
5.2	A Need to Know	17
5.3	Commingling	17
5.4	Access to Federal Tax Return and Return Information Via State Files or Through Other Agencies	18
5.5	Control Over Processing	19
5.6	Computer System Security	20
5.7	Common Criteria	21
5.8	Transmitting Federal Tax Information	22
6.0	**Other Safeguards - IRC 6103(p)(4)(D)**	25
6.1	General	25
6.2	Employee Awareness	25
6.3	Internal Inspections	25

TABLE OF CONTENTS

Section	Title	Page
7.0	**Reporting Requirements - IRC 6103(p)(4)(E)**	27
7.1	General	27
7.2	Safeguard Procedures Report	27
7.3	Submission of Safeguard Procedures Report	29
7.4	Annual Safeguard Activity Report	29
7.5	Submission Dates for the Safeguard Activity Report	30
8.0	**Disposal of Federal Tax Information - IRC 6103(p)(4)(F)**	31
8.1	General	31
8.2	Returning IRS Information to the Source	31
8.3	Destruction Methods	31
8.4	Other Precautions	31
9.0	**Return Information in Statistical Reports - IRC 6103(j)**	33
9.1	General	33
9.2	Making a Request	33
10.0	**Reporting Improper Disclosures IRC 7213, 7213A, 7431**	35
10.1	General	35
11.0	**Disclosure to Other Persons - IRC 6103(n)**	37
11.1	General	37
11.2	Authorized Disclosures	37
11.3	State Tax Officials and State and Local Law Enforcement Agencies	37
11.4	State and Local Child Support Enforcement Agencies	37
11.5	Federal, State, and Local Welfare Agencies	38
11.6	Deficit Reduction Agencies	38
11.7	Health and Human Services	38
11.8	Disclosures Under IRC 6103(m)(2)	38
	Guides	
1		5
2		15
3		24
	Exhibits	
1	IRC 6103(a) and 6103(b)	39
2	IRC 6103(p)(4)	43
3	IRC 7213(a) and 7213A	45
4	IRC 7431	47

TABLE OF CONTENTS

Section	Title	Page
	Exhibits	
5	Contract Language for General Services	49
6	Functional and Assurance Requirements	51
7	Evaluation Assurance Level 3	55
8	Encryption Standards	57

1.1 General

The self-assessment feature is a distinguishing characteristic and principal strength of American tax administration. The IRS is acutely aware that in fostering our system of taxation the public must 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 IRC 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 (FTI). Additionally, IRC 7213A, makes the unauthorized inspection of FTI a misdemeanor punishable by fines, imprisonment, or both. And finally, IRC 7431 prescribes civil damages for unauthorized inspection or disclosure and upon conviction the notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

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.

The sanctions of the IRC 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 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 FTI 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. Additionally, as agencies look more to the "contracting out" of certain services, it becomes equally important that those with whom contracts exist protect that information from unauthorized use, access, and disclosure.

1.2 Overview of Publication 1075

This publication is intended to provide guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS. The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI in electronic form must be afforded the same levels of protection given to paper documents or any other media containing FTI. Security policies and procedures should minimize circumvention.

A mutual interest exists with respect to our responsibility to ensure that FTI 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 Publication 1075 will be helpful. Conformance to these guidelines will meet the safeguard requirements of IRC 6103(p)(4) and make our joint efforts beneficial.

This publication is divided into eleven sections. Following the Introduction, Section 2 addresses most of the preliminary steps an agency should consider before submitting a request to receive FTI. Additionally, it addresses what to expect from the IRS once the information has been disclosed. Sections 3 through 8 are directed toward the requirements of proper safeguarding and use of FTI as prescribed in the IRC. Sections 9 through 11 address miscellaneous topics that may be helpful in setting up your program. Finally, 3 guides and eight exhibits are provided for additional instructions. Publication 1075 can be accessed through the Internet. Go to:

ftp://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf

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

2.1 General

Section 6103 of the IRC is a confidentiality statute and generally prohibits the disclosure of FTI **(see Exhibit 1 for general rule and definitions)**. However, exceptions to the general rule authorize disclosure of FTI 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 or delegate. FTI 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 FTI 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 FTI, 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 use. 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 record keeping 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 FTI **(see Section 7.0 - Reporting Requirements).**

The SPR should include the processing and safeguard procedures for all FTI received and it should distinguish between agency programs and functional organizations using FTI. Multiple organizations or programs using FTI 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 sections of the IRC and for different purposes.

An agency must ensure its safeguards will be ready for immediate implementation upon the receipt of Federal tax information.

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

2.2 Need and Use

Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs FTI for a different authorized use under a different provision of IRC 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 imposition of civil or criminal penalties on the responsible officials. As more states are using contractors to enhance existing systems and processes, they may want to use IRS data in the testing stage prior to going operational. If this is the case, need and use statements should be revised to cover this use of IRS data if not already addressed. State taxing agencies should check their statements (agreements) to see if "testing purposes" is covered.

2.3 State Tax Agencies

FTI 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 FTI 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 FTI on a continuing basis finds it is receiving information that, for any reason, it is unable to use, 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 FTI 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."

2.4 Coordinating Safeguards Within an Agency

Because of the diverse purposes that authorized disclosures may be made to an agency and the division of responsibilities among different, disparate components of an agency, FTI may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of FTI, 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 ensuring that internal inspections are conducted **(see Section 6.0 - Other Safeguards)**, for submitting required safeguard reports to IRS, and for any necessary liaison with IRS.

2.5 Safeguard Reviews

A safeguard review is an on-site evaluation of the use of FTI and the measures employed by the receiving agency to protect that data. This includes FTI received from the IRS, the Social Security Administration (SSA), or other agencies. Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to an evaluation of the agency's programs. 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. Reviews are conducted by the IRS Office of Communications & Liaison, Office of Governmental Liaison & Disclosure.

2.6 Conducting the Review

The Internal Revenue Service initiates the review by verbal communication with an agency point of contact. The preliminary discussion will be followed by a formal engagement letter to the agency head giving official notification of the planned safeguard review. The engagement letter outlines what the review will encompass; for example, it will include a list of records to be reviewed

A safeguard review is an on-site evaluation of the use of Federal tax information received from the IRS, the Social Security Administration, or other agencies and the measures employed by the receiving agency to protect that data.

(e.g., training manuals, flow charts, awareness program documentation and organizational charts relating to the processing of FTI), 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 6103(p)(4). They are Record Keeping, Secure Storage, Restricting Access, Other Safeguards, Reporting Requirements, and Disposal. Computer

Security and Need and Use, as it applies under IRC 6103(d), are a part of Restricting Access but may appear in the report under its own heading. The six requirements are covered in depth in the text of this publication.

Observing actual operations is a required step in the review process. Agency files may be spot checked to determine if they contain FTI. The on-site review officially begins at the opening meeting where procedures and parameters will be communicated. The actual review is followed by a closeout meeting whereby the agency is informed of all findings as a result of the evaluation. An Interim Report will be issued to document the on-site review findings and discussion at the closeout session. Next, the agency will have the opportunity to provide formal comments to the Interim Report. A Final Report will be issued encompassing the interim report, agency comments, and IRS' response to those comments.

Note: All findings should be addressed in a timely fashion. Outstanding issues should be resolved and addressed by the next reporting cycle in the Safeguard Activity Report, or if necessary, the Safeguard Procedures Report **(See Section 7.4.3 - Actions On Safeguard Review Recommendations).**

Guide 1

9 Steps of the Review Process

Preliminary Discussions
Engagement Letter
Opening Meeting
On-site Evaluation
Close-out Meeting
Interim Report
Agency Response
IRS Response
Final Report

3.1 General

Federal, state, and local agencies, bodies, commissions, and agents authorized under IRC 6103, to receive FTI are required by IRC 6103(p)(4)(A) to establish a permanent system of standardized records of requests made, by or to them, for disclosure of FTI **(see Exhibit 2).** This record keeping should include internal request among agency employees as well as request outside of the agency. The records are to be maintained for five years or the applicable records control schedule, whichever is longer.

3.2 Electronic Files

Authorized employees, of the recipient agency must, be responsible for securing magnetic tapes/cartridges before, during, and after 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 FTI, 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:

- date received
- reel/cartridge control number contents
- number of records if available
- movement and
- if disposed of, the date and method of disposition.

Such a log will permit all tapes (including those used only for backup) containing FTI to be readily identified and controlled. Responsible officials must ensure that the removal of tapes and disks (containing FTI) 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.

In instances where auditors read large volumes of records containing Federal tax information, whether in paper or electronic format, the State tax agency need only identify the bulk records examined.

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 FTI and must be afforded the same consideration as other FTI received as a result of the match.

3.3 Information Other Than That In Electronic Form

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

- a taxpayer name
- tax year(s)
- type of information (i.e., revenue agent reports, Form 1040, work papers, etc.)
- the reason for the request
- date requested
- date received
- exact location of the FTI
- who has had access to the data and
- if disposed of, the date and method of disposition.

The agency must account for any missing tape by documenting search efforts and notifying the initiator of the loss.

If the authority to make further disclosures is present (i.e., agents/contractors), 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 FTI from a main frame computer to another main frame computer, as in the case

of the SSA sending FTI 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.

3.4 Record Keeping 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 FTI for further scrutiny and inclusion in their work papers. In instances where auditors read large volumes of records containing FTI, 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, a description of the records, and the name of the individual(s) making the inspection.

4.1 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 that 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.

The IRS has categorized Federal tax and privacy information as High Security items. Guide 2 on page 15 should be used as an aid in determining the method of safeguarding high security items.

4.2 Minimum Protection Standards (MPS)

The Minimum Protection Standards (MPS) system establishes a uniform method of protecting data and items that require safeguarding. This system contains minimum standards that 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 FTI. MPS requires two barriers to accessing FTI under normal security - secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Locked means an area or container that has a lock and the keys or combinations are controlled. A security container is a lockable metal container with a resistance to forced penetration, with a security lock and keys or combinations are controlled. (See section 4.3 for secured perimeter/interior.) The reason for the two barriers is to provide an additional layer of protection to deter, delay or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after hours.

Using a common situation as an example, often an agency desires or requires that security personnel or custodial service workers have access to locked buildings and rooms. This may be permitted as long as there is a second barrier to prevent access to FTI. A security guard may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard or janitor may have a key to the building but not the room.

4.3 Security of Tax Information

Care must be taken to deny access to areas containing FTI during duty hours. This can be accomplished by restricted areas, security rooms, or locked rooms. Additionally, FTI 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.

Restricted Area

A restricted area is an area that entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas must either meet secured area criteria or provisions must be made to store high security 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 FTI.

Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and must have controlled access (electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need enter.

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.

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 of 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 a second level of management review the register. 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.

Security Room

A security room is a room that 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 below in "Locking Systems for Secured Areas and Security Rooms," and entrance limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room.

Additionally, 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 that 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 Interior/Secured Perimeter

Secured areas are internal areas that 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 used, 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.

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.

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.

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.

Safes/Vaults

A safe is a GSA approved container of Class 1, IV, or V, or 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, uses UL approved vault doors, and meets GSA specifications.

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

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). The management should maintain combinations (other than safes and vaults). 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. A periodic reconciliation should be done on all key records.

Locking Systems for Secured Areas and Security Rooms

Minimum requirements for locking systems for Secured Areas and Security Rooms are high security pin-tumbler cylinder locks that 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.

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. Additionally, alarms for individual and document safety (fire) and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site 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.

4.4 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 FTI. 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.

4.5 Handling and Transporting Federal Tax Information

The handling of FTI 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 FTI.

Any time FTI 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 FTI (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 FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. The use of sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof.

4.6 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 FTI 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.

> *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.*

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 3 - Record Keeping Requirements - contains additional information on these requirements.

4.7 Alternate Work Sites

If the confidentiality of FTI can be adequately protected, alternative work sites, such as employees' homes or other non-traditional work sites can be used. Despite location, FTI 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.

Note: Although the guidelines are written for employees' homes, the requirements apply to all alternative work sites.

Equipment

Only agency-owned computers and software will be used to process, access, and store FTI. 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 way to communicate 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.

Despite location, FTI remains subject to the same safeguard requirements and the highest level of attainable security.

The agency should provide "locking hardware" to secure Automated Data Processing 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.

Transmission and Storage of Data

FTI may be stored on hard disks only if agency approved security access control devices (hardware/software) have been installed, is receiving regularly scheduled maintenance, including upgrades, and is being used. Access control should include password security, an audit trail, encryption or guided media, virus detection, and data overwriting capabilities.

Note: Additional information on Remote Access can be found in Section 5.8 - Transmitting Federal Tax Information.

Other Safeguards

Only agency-approved security access control 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, and maintain documentation on the test. Before implementation, the agency will perform both Unit Tests and Acceptance Tests, and will certify that the security controls are adequate for security needs. Additionally, the agency will promulgate rules and procedures to ensure that computers are not left unprotected at 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 7.0 - Reporting Requirements - for details).**

Guide 2

PHYSICAL SECURITY - MINIMUM PROTECTION STANDARDS

ALTERNATIVE 1:

Secured Perimeter - Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection. Any lesser-type partition supplemented by UL approved electronic intrusion detection and fire detection systems. Unless there is electronic intrusion detection devices, all doors entering the space must be locked. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded and the gate must be either guarded or locked with intrusion alarms. Space must be cleaned during duty hours. This requirement could apply to exterior or interior perimeters.

Locked Container - A commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with lockable drawers.

ALTERNATIVE 2:

Locked Perimeter - High security pin-tumbler cylinder locks meeting the following criteria:

key operated mortised or rim-mounted dead bolt lock
dead bolt throw of one inch or longer
double cylinder design - must have five or more pin tumblers
if bolt is visible when locked, must contain hardened inserts or be made of steel
both the key and the lock must be “off master”.

Secured Interior Area - Same specifications as secured perimeter.

ALTERNATIVE 3:

Locked Perimeter - See above.

Security Container - Metal containers that are lockable and have a resistance to penetration. There should only be 2 keys to the containers. Strict control of keys is mandatory. (Ex: mini safes, metal lateral key lock files, metal pull drawer cabinets with center/off center lock bars secured by padlocks).

5.1 General

Agencies are required by IRC 6103(p)(4)(C) to restrict access to FTI only to persons whose duties or responsibilities require access **(see Exhibits 2 and 4)**. To assist with this, FTI 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.

5.2 A Need to Know

Good safeguard practice dictates that access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. Agencies must evaluate the need for FTI 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.

Restricting access to designated personnel minimizes improper disclosure. 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 FTI to the individual who receives it; the official may need to forward FTI to technical and clerical employees for necessary processing. However, no person should be given more FTI than is needed for performance of his or her duties.

Examples:

- When documents are given to a clerk/typist, no FTI should be included unless it is needed for performance of clerical or typing duties.

Good safeguard practice dictates that access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission.

- 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 FTI to do their jobs but do not require access to FTI (e.g., a tape librarian or a computer operator).

5.3 Commingling

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

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

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

controlled by:

- Systemic means, including labeling. **See Section 5.6 - Computer System Security - for additional information.**

- Restricting computer access only to authorized personnel.

- Degaussing all of the data being removed after each use.

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

Examples of commingling:

- If FTI is included in an inquiry or verification letter or in an internal data input form, the FTI never loses its character as FTI even if it is subsequently verified. If the document has both FTI and information provided by the individual or third party, commingling has occurred and the document must also be labeled and safeguarded. If the individual or a third party from their own source provides the information, this is not return information. "Provided" means actually giving the information on a separate document, not just verifying and returning a document that includes return information.

- If a new address is received from Internal Revenue Service records and entered into a computer database, then the address must be identified as FTI and safeguarded. If the individual or third party subsequently pro vides the address, 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.

5.4 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, IRC 6103(d) does not permit access to FTI by such employees, agencies, or other organizations. The IRC clearly provides that FTI 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 FTI, your inquiry should be forwarded to the Disclosure Officer at the IRS District Office that serves your location. The IRC does not permit state tax agencies to furnish FTI to other state agencies, tax or non-tax, or to political sub-divisions, such as cities or counties, for any purpose, including tax administration. Nor may state tax agencies furnish FTI 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 FTI.

The IRC does not permit state tax agencies to furnish FTI to other state agencies, tax or non-tax, or to political sub-divisions, 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 FTI. Generally, statutes that authorize disclosure of FTI do not authorize further disclosures. Unless IRC 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 that the disclosure is authorized, and outside the agency, including contractors or agencies with whom data exchange agreements exist. Agencies may be authorized access to the same FTI for the same purposes, such as state tax agencies, and subdivisions of the same agency may obtain the same type of FTI for different purposes, such as welfare agencies participating in both welfare eligibility verification [IRC 6103(l)(7)] and child support enforcement [IRC 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, i.e., different programs or purposes, each exchange or release of FTI 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 FTI to agents, representatives, or contractors.

5.5 Control Over Processing

Processing of FTI 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 that 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 that processes FTI for tax administration or Federal debt collection purposes. The requirements in Exhibit 5 must be included in the 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 contractor or agency-shared computer facility is also subject to IRS Safeguard Reviews.

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 [IRC 6103(l)(7)] or those with respect to whom child support obligations are sought to be established or enforced pursuant to the provisions of part D of title lV of the Social Security Act [IRC 6103(1)(6)], and the refund offset disclosures [IRC 6103(l)(10)]. Recipients of return information disclosed by the IRS or by SSA under the Deficit Reduction Act are allowed to use a shared facility but only in a manner that does not allow access to FTI 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 media to a private contractor or other agency office even if the purpose is merely to erase the old media for reuse.

5.6 Computer System Security

A good computer security program is based on a strong management framework being in place. It is recommended therefore that agency management take an active role in the security of information assets. This can be accomplished by having a written computer security policy, addressing computer security from a continuing risk management cycle approach, performing independent audits of security controls, and instituting best practices for computer security.

System Security Policy

A computer system security policy is a written document describing the system in terms of categories of data processed, users allowed access, and access rules between users and the data. Establishing a simple computer use policy and communicating that policy to all employees having access to systems and computers housing sensitive data is crucial. Being able to demonstrate to employees that agency officials are aware of user activity on a system and that the agency cares what transpires on and to a system, serves as a first line of defense and a strong deterrent against unauthorized access and use.

Access to FTI must be controlled on a need-to-know basis. Agencies which receive FTI are required to plan and implement controls which enforce "need-to-know" access. Required controls include

- unique identification and authentication of users,
- control of user access to data and system resources,
- an audit trail (maintain current year and 5 prior years) of user activities to ensure that user actions are within established controls, and
- protection of residual data from unauthorized access.

These four control categories support individual accountability. When developing and implementing policy controls, consideration must be given to aspects of network and other communication topologies, as well as system administration functions. Agencies must document controls in a security policy which describes the controls and how they work to protect need-to-know access to FTI.

Note: Controls are not limited to the technical and logical environment. Physical, administrative, and operational (e.g., procedural) controls may be necessary. Moreover, implemented control mechanisms must be coordinated to achieve the overall objective of FTI protection. Individuals responsible for system operations must be trained in the installation and use of the control mechanisms, and explicitly made responsible for their correct installation and maintenance.

After setting appropriate controls, an agency must methodically consider security as part of normal network operations. This could be as simple as configuring routers to not accept unauthorized addresses or services, or as complex as installing firewalls, intrusion detection systems, centralized authentication servers, and encryption.

A basic tenet of military combat engineers is that an unobserved obstacle will eventually be breached. The same is true in computer system networks. Unauthorized users will eventually figure out a way around static defenses. The number and frequency of computer attacks is constantly on the rise. As such, a critical part of computer security is to monitor one's network infrastructure and then respond to attempted or successful attacks. Agencies should scan their own networks regularly, updating electronic network maps, determining what hosts and services are running, and cataloging vulnerabilities.

Risk Management

The risk management approach involves

identifying, assessing, and understanding information security risks to program operations and assets, identifying related needs for protection, selecting and implementing controls that meet these needs, promoting continuing awareness and responsibility, and implementing a program for routinely testing and evaluating policy and control effectiveness.

Independent Audits

Annual independent audits prove to be effective in an agency's information security program. Tests and evaluations are essential in verifying the effectiveness of computer based controls. They evaluate agency implementation of management initiatives, thus promoting management accountability, and they identify both obstacles and progress toward improving information security. It is recommended that an independent test be used to validate that the control mechanisms

- adequately address security needs,
- are properly installed, and
- operate as designed in the installed environment

Agencies could bring in experts to conduct independent network security posture audits once or twice a year to provide a more thorough assessment of threats and vulnerabilities and to get independent, outside recommendations regarding countermeasures, security patches, and other improvements. Experts can not access Federal tax information unless authorized by statute, **see Section 11 Disclosure to Other Persons.**

Best Practice

Finally, there must be a feedback loop in every "best practice." System administrators must be empowered to make improvements. Senior management must be held accountable for network security, and those involved in day-to-day operations must have their attention. Only by collecting and managing appropriate network security data, through audit logs, intrusion detection and response systems, and network scans, can management make intelligent decisions towards maintaining and improving computer security.

5.7 Common Criteria

In 1999, a new standard for identifying and evaluating security features was adopted. This new standard, Common Criteria for Information Technology Security Evaluation (CCITSE), usually referred to as the Common Criteria (CC), ISO/IEC 15408, replaces the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) (DoD 5200.28-STD), or the Orange Book.

The Common Criteria differs from the TCSEC in its standardization approach. The TCSEC defined the specific security functionalities which must exist and the specific testing which must be performed to verify the security functionalities were implemented correctly (i.e. assurance) in predefined classes such as C2. Conversely, the Common Criteria is more of a lexicon or language which provides a standardized and comprehensive list of security functionalities and analysis techniques which may be performed to verify proper implementation, as well as a common evaluation methodology to perform the tests. The greater the degree of analysis, the higher the assurance that the product performs as advertised.

The National Security Agency has already translated the TCSEC "C2" class for operating systems into the Common Criteria-based specifications or "Protection Profile." Guide 3, page 24, compares the TCSEC and the CC and should help with understanding the migration. For a further explanation of CC terms see Exhibits 6 and 7.

Note: Effective October 1, 1999, all agencies that receive, process, store, or transmit FTI are encouraged to identify protection requirements for FTI using the Common Criteria. More information about CC can be obtained at

http://csrc.nist.gov/cc.

Agencies installing new equipment to comply with the C2 requirement prior to October 1, 1999 will be granted a **temporary waiver**. However, by the end of 2001 all products which were previously evaluated against the C2 rating shall be migrated to the Common Criteria evaluation rating.

5.8 Transmitting Federal Tax Information

The two acceptable methods of transmitting FTI over telecommunication devices are the use of encryption or 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).**

Unencrypted cable circuits of copper or fiber optics is an acceptable means of transmitting FTI. Measures are to be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. Additional precautions should be taken to protect the cable, (e.g., burying the cable underground or in walls or floors and providing access controls to cable vaults, rooms and switching centers).

Note: Employing intrusion detection devices, auditing capability with periodic monitoring, and other security measures will further reduce threats and vulnerabilities when using this (guided media) method of transmitting sensitive data.

Remote Access

Accessing databases containing FTI from a remote location - i.e., a location not directly connected to the Local Area Network - will require adequate safeguards to prevent unauthorized entry. The IRS policy for allowing access to systems containing FTI is outlined below.

- Authentication is provided through ID and password encryption for use over public telephone lines.
- Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.
- Standard access is provided through a toll - free number and through local telephone numbers to local data facilities.
- Both access methods (toll free and local numbers) require the purchase of a special (encrypted) modem for every workstation and a smart card (microprocessor) for every user. Smart cards should have both identification and authentication features and provide data encryption as well.

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 that adequate security measures are employed to restrict access to sensitive data. **See section 5.6 Computer System Security.**

Electronic Mail

Generally, FTI should not be transmitted or used on E-mail systems. If necessary, precautions should be taken to protect FTI sent via E-mail.

- Do not send FTI in the text of the E-mail.

- Messages containing FTI must be attached and encrypted.

- Ensure that all messages sent are to the proper address and

- Employees should log off the computer when away from the area.

Note: At the time of this publication, IRS was drafting new controls for the electronic transmission of FTI using E-mail.

Facsimile Machines (Fax)

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

- Have a trusted staff member at both the sending and receiving fax machines, or have a locked room for the fax machine with custodial coverage over outgoing and incoming transmissions.

- Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI. Place fax machines in a secured area.

- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:

  --A notification of the sensitivity of the data and the need for protection and

  --A notice to unintended recipients to telephone the sender - collect if necessary - to report the disclosure and confirm destruction of the information.

ISO/IEC 15408 STD - Common Criteria (18)	DoD 5200.28 - C2 (14)
Security Audit	Auditing
Communications	Communication Infrastructure
Cryptographic support	Encryption Methodology
User data protection	Discretionary Access Control Object Reuse
Identification and authentication	Identification and Authentication
Security management	Discretionary Access Control Object Reuse Trusted Computing Base
Privacy	Trusted Facility Manual
Protection of the TOE	Trusted Computing Base (TCB) System Architecture System Integrity
Resource Utilization	Trusted Facility Manual
TOE Access	Authentication
Trusted Path/Channels	Communications Infrastructure Discretionary Access Controls
Configuration Management	Security Testing Design Documentation
Delivery and Operation	Trusted Facility Manual
Development	Design documentation
Guidance Documentation	Security Function User's Guide
Life Cycle Support	Security Testing
Tests	Security Testing Test Documentation
Vulnerability Assessment	Auditing Security Testing

6.1 General

IRC 6103(p)(4)(D) requires that agencies receiving FTI provide other safeguard measures as appropriate to ensure the confidentiality of the FTI. A good security awareness program is by far the most effective least expensive method agencies can use to protect sensitive information.

6.2 Employee Awareness

Granting agency employees access to FTI should be preceded by certifying that each employee understands the agency's security policy and procedures for safeguarding IRS information. As a follow up, employees should be required to maintain their authorization to access FTI 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 7213(a), 7213A, and 7431 **(see Exhibits 3 and 4).**

Note: Agencies should make employees aware that disclosure restrictions and the penalties apply even after employment with the agency has ended.

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

- Formal and informal training.
- Discussion at group and managerial meetings.
- Install security bulletin boards throughout the work areas.
- Place security articles in employee newsletters.
- Route pertinent articles that appear in the technical or popular press to members of the management staff.
- Display posters with short simple educational messages (e.g., instructions on reporting UNAX violations, address, and hotline number).
- Using warning banners on computer screens housing FTI.
- E-mail and other electronic messages can be sent to inform users.

6.3 Internal Inspections

Another measure required by the IRS is Internal Inspections by the recipient agency. The purpose is to ensure that adequate safeguard 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 7.4 - Annual Safeguard Activity Report)**. To provide an objective assessment, the inspection should be conducted by a function other than the using function.

It should be certified that employees understand security policy and procedures requiring their awareness and compliance.

To provide reasonable assurance that FTI 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:

Record Keeping

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.

Secure Storage

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

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.

Disposal

Upon completion of use, agencies should ensure that the FTI is destroyed or returned to the IRS or the SSA according to the guidelines contained in Section 8.0 - Disposal of Federal Tax Information.

Computer Security

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

- 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 **(see Section 5.6 - Computer Security).**

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

Note: The review of the computer facility should also include computer security.

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.

7.1 General

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

Annually thereafter, the agency must file a Safeguard Activity Report (SAR). This report, 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 FTI, and finally, certifies that the agency is protecting FTI pursuant to IRC 6103(p)(4) and the agency's own security requirements.

Note: Agencies are requested to submit a new SPR every six years or whenever significant changes occur in their safeguard program.

7.2 Safeguard Procedures Report

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

Responsible Officer(s)

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

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

Location of the Data

An organizational chart or narrative description of the receiving agency, that includes all functions within the agency where FTI will be processed or maintained. If the information is to be used or processed by more than one function, then the pertinent information must be included for each function.

The Safeguard Procedures Report 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.

Flow of the Data

A chart or narrative describing the flow of FTI through the agency from its receipt through its return to the IRS or its destruction, how it is used or processed, and how it is protected along the way. (See specific safeguard requirements below.) Indicate if FTI is commingled or transcribed into data kept by the agency. Any data turned over to an agency contractor for processing must be fully disclosed and accounted for.

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 FTI (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 or media.

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 considerations as locked files or containers, secured facilities, key or combination controls, off-site storage, and restricted areas.

Note: It is requested that **Federal Agencies** submit a Vulnerability Assessment based on General Services Administration standards for their building(s) as it addresses physical security.

Restricting Access to the Data

A description of the procedures or safeguards employed to ensure access to FTI 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 FTI is used or processed) and systemic or procedural barriers.

Disposal

A description of the method(s) of disposal of the different types of FTI provided by the IRS when not returned to the IRS. The IRS will request a written report that documents the method of destruction and the that records were destroyed . (See "4" above.)

Computer Security

All automated information systems and networks that receive, process, store, or transmit sensitive but unclassified information (FTI), must have adequate safeguard measures in place to restrict access to sensitive data **(see Section 5.6 - Computer Security and Section 5.7 - Common Criteria).** These safeguards should address each applicable tier level.

A. Microprocessors and Mainframe Systems (Tier I)

Describe the systemic controls employed to ensure all IRS 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.

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

B. Local and Wide Area Networks, Internet, etc. (Tier II)

Describe in detail the security precautions undertaken if the agency's computer systems are connected or planned to be connected to other systems.

C. Personal Computer/Notebook/Laptops (Tier III)

In the event that FTI is (or is likely to be) used or processed by agency employees on personal computers, the Safeguard Procedures Report must include 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.

Agency Disclosure Awareness Program

Each agency receiving FTI should have an awareness program that annually notifies all employees having access to FTI of the confidentiality provisions of the IRC, 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.

7.3 Submission of Safeguard Procedures Report

Federal, Child Support Enforcement, and State Welfare agencies requesting FTI should submit their report to:

National Director
Governmental Liaison and Disclosure
OP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224
E-mail: SafeguardReports@irs.gov

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

7.4 Annual Safeguard Activity Report

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

Changes to Information or Procedures Previously Reported

A. Responsible Officers or Employees

B. Functional Organizations Using the Data

C. Computer Facilities or Equipment and System Security - Changes or Enhancements

D. Physical Security - Changes or Enhancements

E. Retention or Disposal Policy or Methods

Current Annual Period Safeguard Activities

A. Agency Disclosure Awareness Program

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

B. Reports of Internal Inspections

Copies of a representative sampling 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.

C. Disposal of FTI

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

Note: Including taxpayer information in the disposal record is not necessary and should be avoided.

Actions on Safeguard Review Recommendations

The agency should report all actions taken, or being initiated, regarding recommendations in the Final Safeguard Review Report issued as a result of the latest safeguard review.

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.

Agency Use of Contractors

Agencies must account for the use of all contractors, permitted by law or regulation, to do programming, processing, or administrative services requiring access to FTI.

7.5 Submission Dates for the Safeguard Activity Report

Federal Agencies should submit their reports for the calendar year by January 31 of the following year to: (See address below)

Law Enforcement Agencies receiving 8300 Information should submit their reports for the processing year (May 1 through April 30) by June 30 to: (See address below)

State Welfare Agencies and DC Retirement Board should submit their reports for the processing year (July 1 through June 30) by September 30 to: (See address below)

State Child Support Enforcement Agencies should submit their reports for the calendar year by January 31 of the following year to:

National Director
Governmental Liaison and Disclosure
OP:EX:GLD
ATTN: Office of Safeguards
1111 Constitution Avenue, NW
Washington, DC 20224
E-mail: SafeguardReports@irs.gov

Note: Federal agencies receiving FTI under IRC 6103(m)(4)(B) should send reports to the oversight agency.

State Tax Agencies should submit their reports 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.

8.1 General

Users of FTI are required by IRC 6103(p)(4)(F) to take certain actions upon completion of use of Federal tax information in order to protect its confidentiality **(see Exhibits 2 and 4).** Agency officials and employees will either return the information (including any copies made) to the office that it was originally obtained or make the information "undisclosable." Agencies will include in their annual report (SAR) a description of the procedures used.

8.2 Returning IRS Information to the Source

Agencies electing to return IRS information, must use a receipt process and ensure that the confidentiality is protected at all times during transport **(see Section 4.5 - Handling and Transporting Federal Tax Information).**

8.3 Destruction Methods

FTI furnished to the user and any material generated therefrom, 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.

The following precautions should be observed when destroying FTI:

- 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 and not maintain small amounts of shredded paper. 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. If shredding is part of the overall destruction of IRS data, strips can in effect be set at the industry standard (currently ½"). However, when deviating from IRS' 5/16" requirement, IRS data, as long as it is in this condition (i.e., strips larger than 5/16"), must be safeguarded until it reaches the stage where it is rendered unreadable.

- Pulping should be accomplished so that all material is reduced to particles one inch or smaller.

8.4 Other Precautions

FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee. 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)- l. The required safeguard language is contained in Exhibit 5. If this method is used, it is recommended that periodically the agency observe the process to ensure compliance. Destruction of FTI should be certified by the contractor when agency participation is not present.

Magnetic tape containing FTI 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 FTI 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, recycling, or burying information in a landfill are unacceptable methods of disposal.

9.1 General

IRC 6103 authorizes the disclosure of FTI for use in statistical reports, for tax administration purposes, and certain other purposes specified in IRC 6103(j). However, such statistical reports may only be released in a form that 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 that has been approved by the IRS:

- Access to FTI 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 10 returns, and
- Tabulations that would pertain to specifically identified taxpayers or that would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

9.2 Making a Request

Agencies and organizations seeking statistical information from IRS should make their requests under IRC Section 6103(j). The requests should be addressed to:

Director, Statistics of Income Division; OP:S Internal Revenue Service, 1111 Constitution Avenue, NW. Washington, DC 20224.

10.1 General

Upon discovery of a possible improper inspection or disclosure of FTI 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 Special Agent-in-Charge, Treasury Inspector General for Tax Administration.

Field Division	States Served by Field Division	Telephone Number
Atlanta	Alabama, Arkansas, Georgia, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee	(404) 338-7400
Boston	Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont	(617) 565-7750
Chicago	Illinois, Iowa, Kansas, Minnesota, Missouri, North Dakota, South Dakota, Wisconsin, Nebraska	(312) 886-0533
Cincinnati	Indiana, Kentucky, Ohio, Michigan, West Virginia	(513) 263-3040
Dallas	Oklahoma, Texas	(972) 308-1400
Denver	Arizona, Colorado, Idaho, Montana, New Mexico, Nevada, Utah, Wyoming	(303) 446-1880
Jacksonville	Florida	(904) 665-1185
Los Angeles	Southern California	(213) 894-4527
New York	New York	(212) 637-6800
Philadelphia	New Jersey, Pennsylvania	(215) 861-1000
San Francisco	Alaska, Hawaii, Northern California, Oregon, Washington	(510) 637-2558
Washington	Delaware, Maryland, Virginia, Washington DC	(202) 283-3000
Special Inquiries and Inspection	Commonwealth of Puerto Rico, Virgin Islands, Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	(703) 812-1688

Mailing Address: **Treasury Inspector General for Tax Administration**
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589

Hotline Number: **1-800-366-4484**

11.1 General

Disclosure of FTI is generally prohibited unless authorized by statute. Agencies having access to FTI are not allowed to make further disclosures of that information to their agents or to a contractor unless authorized by statute. The terms agent and contractor are not synonymous. Agencies are encourage to use specific language in their contractual agreements to avoid ambivalence or ambiguity.

Note: Absent specific language in the IRC or where the IRC is silent in authorizing an agency to make further disclosures, IRS' position is that further disclosures are unauthorized.

11.2 Authorized Disclosures - Precautions

When disclosure is authorized certain precautions should be taken by the agency prior to engaging a contractor, namely:

- Has the IRS been given sufficient prior notice before releasing information to a contractor?
- Has the agency been given reasonable assurance through an on-site visitation or received a report certifying that all security standards (physical and computer) have been addressed?
- Does the contract requiring the disclosure of FTI have the appropriate safeguard language **(see Exhibit 5 Contract Language for General Services)**?

Agencies should fully report to the IRS all disclosures of IRS information to contractors in their Safeguard Procedures Report. Additional disclosures to contractors should be reported on the annual Safeguard Activity Report.

The engagement of a contractor who may have incidental or inadvertent access to FTI does not come under these requirements. Only those contractors whose work will involve the disclosure of FTI in the performance of their duties are required to address these issues.

11.3 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 FTI. **See Section 5.4 Access to Federal Tax Information via State Tax Files or Through Other Agencies for additional information.**

11.4 State and Local Child Support Enforcement Agencies IRC 6103(1)(6)

In general, no officer or employee of any state and local child support enforcement agency can make further disclosures of FTI. However, the Welfare Reform Act of 1997 gave authorization to disclose limited information to agents or 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 or a contractor 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 any reduction under section 6402(c) in any overpayment otherwise payable to such individual.

Note: 1099 and W-2 information is not authorized by statute to be disclosed to contractors under the IRC 6103(1)(6) program.

11.5 Federal, State, and Local Welfare Agencies IRC 6103(1)(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 FTI.

Note: 1099 and W-2 information is not authorized by statute to be disclosed to contractors under the IRC 6103(1)(7) program.

11.6 Deficit Reduction Agencies IRC 6103(1)(10)

Agencies receiving FTI under deficit reduction IRC 6402(c) and IRC 6402(d) are prohibited from making further disclosures to contractors.

11.7 Health Care Financing Administration IRC 6103(l)(12)(C)

Health Care Financing Administration (HCFA) is authorized under IRC 6103(l)(12) to disclose FTI it receives from SSA to its agents for the purpose of, and to the extent necessary in, determining the extent that any medicare beneficiary is covered under any group health plan. A contract relationship must exist between HCFA and the agent. The agent however, is not authorized to make further disclosures of IRS information.

11.8 Disclosures Under IRC 6103(m)(2)

Disclosures to agents of a Federal agency under IRC 6103(m)(2) are authorized for the purposes of locating individuals in collecting or compromising a Federal claim against the taxpayer in accordance with sections 3711, 3717, and 3718 of Title 31.

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 (1)(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 (c)(1)(D)(iii), paragraph (6) or (12) of subsection (1), paragraph (2) or (4)(B) of subsection (in), 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)(5), (i)(1), (2), (3), or (5), (j)(1), (2), or (5), (k)(8), (1)(1), (2), (3), (5), (10), (11), (13), (14), (15), or (17) or (o)(1), the General Accounting Office, or any agency, body, or commission described in subsection (d), (i)(3) (B)(i) or (1)(6), (7), (8), (9), (12) or (15), or (16), or any other person described in subsection (l)(16) 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, to 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)(i), or (1)(6), (7), (8), (9) or (16) or any other person described in subsection (l)(16) 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)(5), (i)(1), (2), (3), or (5), (j)(1), (2), or (5), (1)(1), (2), (3), (5), (10), (11), (12), (13), (14), (15), or (17), or (o)(1), or the General Accounting Office, either-

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

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

(3) 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 including an agency or any other person described in subsection (l)(16) or the General Accounting Office has failed to, or does not, meet requirements of this paragraph, he may, after any proceedings for review established 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 including an agency or any other person described in subsection (l)(16) 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), 12(B) or (16) of subsection (1) and which discloses any such information to any agent or any person including an agent described in subsection (l)(16) this paragraph shall apply to such agency and each such agent or other person (except that, in the case of an agent, or any person including an agent described in subsection (l)(16), 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 114(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 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (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(l)] 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 $1000, 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 GENERAL SERVICES

I. PERFORMANCE

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) All computer systems processing, storing, or transmitting Federal tax information must meet ISO STD 15408, called common criteria - functional (Protection Profile) and assurance (EAL). To meet functional and assurance requirements, the operating security features of the system must have the following minimum requirements: a security policy, accountability, assurance, and documentation. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

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

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

(10) (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)-1.

(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 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 **[United States for federal employees]** in an amount equal to the sum of the greater of $1,000 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 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.

FUNCTIONAL REQUIREMENTS

Class FAU: Security audit

Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities (i.e. activities controlled by the Target of Evaluation (TOE) Security Procedures (TSP). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.

Class FCO: Communication

This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt). These families ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.

Class FCS: Cryptographic support

The Target of Evaluation Security Function (TSF) may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

The FCS class is composed of two families: FCS_CKM Cryptographic key management and FCS_COP Cryptographic operation. The FCS_CKM family addresses the management aspects of cryptographic keys, while the FCS_COP family is concerned with the operational use of those cryptographic keys.

Class FDP: User data protection

This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data. FDP is split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

Class FIA: Identification and authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity.

Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g., identity, groups, roles, security or integrity levels).

The unambiguous identification of authorized users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies. The families in this class deal with determining and verifying the identity of users, determining their authority to interact with the TOE, and with the correct association of security attributes for each authorized user. Other classes of requirements (e.g. User Data Protection, Security Audit) are dependent upon correct identification and authentication of users in order to be effective.

Class FMT: Security management

This class is intended to specify the management of several aspects of the TSF: security attributes, TSF data and functions. The different management roles and their interaction, such as separation of capability, can be specified.

Class FPR: Privacy

This class contains privacy requirements. These requirements provide a user protection against discovery and misuse of identity by other users.

Class FPT: Protection of the TSF

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that provide the TSF (independent of TSP-specifics) and to the integrity of TSF data (independent of the specific contents of the TSP data). In some sense, families in this class may appear to duplicate components in the FDP (User data protection) class; they may even be implemented using the same mechanisms. However, FDP focuses on user data protection, while FPT focuses on TSF data protection. In fact, components from the FPT class are necessary to provide requirements that the SFPs in the TOE cannot be tampered with or bypassed.

Class FRU: Resource utilization

This class provides three families that support the availability of required resources such as processing capability and/or storage capacity. The family Fault Tolerance provides protection against unavailability of capabilities caused by failure of the TOE. The family Priority of Service ensures that the resources will be allocated to the more important or time-critical tasks and cannot be monopolized by lower priority tasks. The family Resource Allocation provides limits on the use of available resources, therefore preventing users from monopolizing the resources.

Class FTA: TOE access

This family specifies functional requirements for controlling the establishment of a user's session.

Class FTP: Trusted path/channels

Families in this class provide requirements for a trusted communication path between users and the TSF, and for a trusted communication channel between the TSF and other trusted IT products. Trusted paths and channels have the following general characteristics:

- The communications path is constructed using internal and external communications channels (as appropriate for the component) that isolate an identified subset of TSF data and commands from the remainder of the TSF and user data.

- Use of the communications path may be initiated by the user and/or the TSF (as appropriate for the component)

- The communications path is capable of providing assurance that the user is communicating with the correct TSF, and that the TSF is communicating with the correct user (as appropriate for the component)

In this paradigm, a ***trusted channel*** is a communication channel that may be initiated by either side of the channel, and provides non-repudiation characteristics with respect to the identity of the sides of the channel.

A ***trusted path*** provides a means for users to perform functions through an assured direct interaction with the TSF. Trusted path is usually desired for user actions such as initial identification and/or authentication, but may also be desired at other times during a user's session. Trusted path exchanges may be initiated by a user or the TSF. User responses via the trusted path are guaranteed to be protected from modification by or disclosure to untrusted applications.

ASSURANCE REQUIREMENTS

Class ACM: Configuration management

Configuration management (CM) helps to ensure that the integrity of the TOE is preserved, by requiring discipline and control in the processes of refinement and modification of the TOE and other related information. CM prevents unauthorized modifications, additions, or deletions to the TOE, thus providing assurance that the TOE and documentation used for evaluation are the ones prepared for distribution.

Class ADO: Delivery and operation

Assurance class ADO defines requirements for the measures, procedures, and standards concerned with secure delivery, installation, and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up, and operation.

Class ADV: Development

Assurance class ADV defines requirements for the stepwise refinement of the TSF from the TOE summary specification in the ST down to the actual implementation. Each of the resulting TSF representations provide information to help the evaluator determine whether the functional requirements of the TOE have been met.

Class AGD: Guidance documents

Assurance class AGD defines requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and for administrators, is an important factor in the secure operation of the TOE.

Class ALC: Life cycle support

Assurance class ALC defines requirements for assurance through the adoption of a well defined life-cycle model for all the steps of the TOE development, including flaw remediation procedures and policies, correct use of tools and techniques and the security measures used to protect the development environment.

Class ATE: Tests

Assurance class ATE states testing requirements that demonstrate that the TSF satisfies the TOE security functional requirements.

Class AVA: Vulnerability assessment

Assurance class AVA defines requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

EXHIBIT 7

Evaluation Assurance Level 3

Assurance class	Assurance components
Class ACM: Configuration management	**ACM_CAP.3 Authorization controls** ACM_SCP.1 TOE CM coverage
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures ADO_IGS. 1 Installation, generation, and start-up procedures ADV FSP.1 Informal functional specification
Class ADV: Development	**ADV_HLD.2 Security enforcing high-level design** ADV_RCR. 1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.I User guidance
Class ALC: Life cycle support	**ALC_DVS.1 Identification of security measures**
Class ATE: Tests	**ATE_COV.2 Analysis of coverage** **ATE_DPT.1 Testing: high-level design** ATE_FUN 1 Functional testing ATE_IND.2 Independent testing - sample
Class AVA Vulnerability assessment	**AVA_MSU.1 Examination of guidance** AVA_SOF. 1 Strength of TOE security function evaluation AVA_VLA. 1 Developer vulnerability analysis

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
www.irs.gov
Publication 1075 (Rev. 6-2000)
Catalog Number 46937O