# PUBLICATION 1075

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

***Safeguards for Protecting Federal Tax Returns and Return Information***

**TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE, AND LOCAL AGENCIES AND ENTITIES OMB No. 1545-0962**

Paperwork Reduction Act Notice

The Internal Revenue Service (IRS) asks for the information in the Safeguard Procedures Report and the Safeguard Activity Report to carry out the requirements of the Internal Revenue Code (IRC) Section 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 Office of Management and Budget (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, Federal Tax Returns and return information are confidential, as required by IRC Section 6103.

The information is used by the IRS to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the confidentiality of Federal Tax Information (FTI). 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 any 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 us at:

Tax Products Coordinating Committee
Internal Revenue Service, SE:W:CAR:MP:T:T:SP
1111 Constitution Avenue, NW, IR-6406
Washington, DC. 20224

*Preface*
This publication revises and supersedes Publication 1075 (February 2007).

This page left intentionally blank.

## HIGHLIGHTS FOR 2007

### COMPUTER SECURITY CONTROLS

This document provides updated requirements using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. In addition, this document contains updated controls to include testing of the computer security controls, and additional physical and personnel security controls based on NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, for the moderate impact level.

Note: While the Safeguards Office has responsibility to ensure the protection of Federal Tax Information, it is the responsibility of the organization to build in effective security controls into their own Information Technology (IT) infrastructures to ensure that this information is protected at all points where Federal Tax Information (FTI) is stored and/or maintained. It will not be the intent of IRS to monitor each control identified but to provide these to the organization, identifying those controls required for the protection of moderate risk systems within the federal government.

### SUBMITTING REPORTS AND CORRESPONDENCE

All correspondence, reports, attachments, etc., should be emailed to the Safeguard mailbox using IRS approved encryption:

SafeguardReports@irs.gov.

### INTERNET ACCESS

Agencies can access Publication 1075 on the Internet by going to http://www.irs.gov and searching for “publication 1075.”

### REPORTING UNAUTHORIZED DISCLOSURES

Unauthorized inspection or disclosure of Federal tax information, including breeches and security incidents, must be reported to the appropriate Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA).

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**

### APPEAL PROCESS RELATED TO POSSIBLE SUSPENSION AND/OR TERMINATION OF TAX DATA

Title 26 U. S. Code Section 6103(p)(4) requires external agencies and other authorized recipients of Federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive. That provision of the Code also authorizes the Internal Revenue Service (IRS) to take actions, including suspending or terminating FTI disclosures to any external agencies and other authorized recipients, if there is misuse and/or inadequate safeguards in place to protect the confidentiality of the information. New temporary Federal tax regulation 26 CFR 301.6103(p)(7)-1T establishes a consistent appeal process for all authorized recipients of FTI. See Exhibit 1, *Federal Register*.

### SECURE DATA TRANSFER

Secure Data Transfer (SDT) is an IRS approved process for exchanging data with trading partners. SDT provides encrypted electronic transmission of IRS files to external agencies.

This page left intentionally blank

.

**TABLE OF CONTENTS**

This page left intentionally blank

### *1.1 General*

The self-assessment feature is a distinguishing characteristic and principal strength of American tax administration. The Internal Revenue Service (IRS) is acutely aware that in fostering our system of taxation, the public must 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 Section 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 Section 7213A makes the unauthorized inspection of FTI a misdemeanor punishable by fines, imprisonment, or both. And finally, IRC Section 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 we use to protect the confidential information entrusted to us.

Those agencies or agents that receive FTI directly from either the IRS or from secondary sources (e.g., Health and Human Services, Federal entitlement and lending agencies) must have adequate programs in place to protect the data received. Furthermore, as agencies look more to “contracting out” 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 provides 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.

Enterprise security policies shall address the purpose, scope, responsibilities, and management commitment to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that should be implemented.

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 – systemic, procedural or manual – should minimize circumvention.

A mutual interest exists in 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.

Conforming to these guidelines meets the safeguard requirements of IRC Section 6103(p)(4) and makes our joint efforts beneficial.

This publication provides the preliminary steps to consider before submitting a request to process FTI, provides requirements to properly safeguard information, explains what to expect from the IRS once the information has been disclosed, and suggests miscellaneous topics that may be helpful in setting up your program. Exhibits 1 through 12 are provided for additional guidance.

Publication 1075 can be accessed through the Internet at www.irs.gov.

### *2.1 General*

Section 6103 of the IRC is a confidentiality statute and generally prohibits the disclosure of FTI (see Exhibit 2, *Confidentiality and Disclosure of Returns and Return Information, 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 receipt of FTI. 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 an 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. Each Federal, State, and Local agency 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 receipt of FTI*. Enterprise security p*olicies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls.*

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 Section 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 and/or criminal penalties on the responsible officials. Because more states are using contractors to enhance existing systems and processes, they may want to use IRS

data in the testing stage before implementation. In this 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 Obtaining FTI*

The IRS has established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners. This method is the approved method of receiving information and replaces the tape transfer process.

### *2.4 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 requests should include some account of the result of its use (e.g., disposition of closed cases and summary of revenues generated) or include reasons why the information was not used. If any agency continually receives FTI that for any reason it is unable to use, it should contact the IRS official liaison with respect to 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 "Need and Use" reviews in conjunction with the on-site Safeguard review.

### *2.5 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 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 hold a position high enough in the agency's organizational structure to ensure compliance with the agency 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 the IRS, and for any necessary liaison with the IRS.

### *2.6 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 the 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 evaluating an agency's programs. IRS regularly conducts on-site reviews of agency safeguards. Several factors will be considered when determining the need for and the frequency of reviews. Reviews are conducted by the Office of Safeguards, within the Communication, Liaison, and Disclosure Office (CLD:S).

### *2.7 Conducting the Review*

The IRS 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.

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

The engagement letter outlines what the review will encompass; for example, it will include a list of records to be reviewed (e.g., training manuals, flowcharts, 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 Section 6103(p)(4): Record Keeping, Secure Storage, Restricting Access, Other Safeguards, Reporting Requirements, and Disposal. Computer Security and Need and Use, as it applies under IRC Section 6103(d) are a part of Restricting Access but may appear in the report under their own headings. The six requirements are covered in depth in this publication.

The on-site review officially begins at the opening meeting where procedures and parameters will be communicated. Observing actual operations is a required step in the review process. Agency files may be spot-checked to determine if they contain FTI. The actual review is followed by a close-out meeting when the agency is informed of all findings because of the evaluation. An interim report will be issued to document the on-site review findings and 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***

**Eight Steps of the Review Process**

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

### *3.1 General*

Federal, State, and local agencies, bodies, commissions, and agents authorized under IRC Section 6103 to receive FTI are required by IRC Section 6103(p)(4)(A) to establish a permanent system of standardized records of requests made by or to them for disclosure of FTI (see Exhibit 3, *Sec 6103(p)(4) Safeguards*). This record keeping should include internal requests among agency employees as well as requests outside of the agency. The records are to be maintained for five years or the applicable records control schedule must be followed, whichever is longer.

### *3.2 Electronic Files*

Authorized employees of the recipient agency must be responsible for electronic media before, during, and after processing. Inventory records must be maintained for purposes of control and accountability. Any media containing FTI or any file resulting from the processing will be recorded in a log that identifies:

- date received
- control number and/or file name & contents
- recipient
- number of records, if available
- movement and
- if disposed of, the date and method of disposition.

Such a log will permit all media (including those used only for backup) containing FTI to be readily identified and controlled.

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

Responsible officials must ensure that removal media containing FTI from the storage area is properly recorded on charge-out records. Semiannual inventories of removable media must be conducted. The agency must account for any missing media by documenting search efforts and notifying the initiator of the loss.

### *3.3 Non-electronic Files*

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

- taxpayer name
- tax year(s)
- type of information (e.g., revenue agent reports, Form 1040, work papers)
- 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 media. This includes documenting the incident and search efforts and notifying the initiator of the loss.*

If the authority to make further disclosures is present (e.g., 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 one mainframe computer to another, as in the case of the SSA sending FTI to State Welfare and in instances where the auditors extract FTI for Child Support agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of the transmissions, 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 utilize 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 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*

Security may be provided for a document, an item, or an area in a number of ways. 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 moderate risk. Guide 2, Physical Security – Minimum Protection Standards, within this document, should be used as an aid in determining the method of safeguarding highly sensitive items. These controls are intended to protect the systems that contain FTI. It is not the intent of the IRS to mandate requirements to those systems and/or areas that are not processing FTI.

### *4.2 Minimum Protection Standards (MPS)*

The Minimum Protection Standards (MPS) establish 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 access 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 4.3.4 for secured perimeter/interior.) The two barriers 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.

Additional controls have been integrated into this document that map to guidance received from the National Institute of Standards & Technology (NIST). These are identified in Exhibit 4, *NIST Moderate Risk Controls for Federal Information Systems.* Through this document, the exhibit will simply be referenced as Exhibit 4.

Policies and procedures shall be developed, documented, and disseminated, as necessary, to facilitate implementing physical and environmental protection controls. (Exhibit 4 PE-1).

### *4.3 Security of Tax Information*

Care must be taken to deny unauthorized access to areas containing FTI during duty and non-duty hours. This can be accomplished by creating 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.

### *4.3.1 Restricted Area*

A restricted area is an area that entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas either must meet secured area criteria or provisions must be made to store high security items in appropriate containers during non-duty hours. Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access and/or disclosure or theft of FTI. All of the following procedures must be implemented to qualify as a restricted area.

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.

*Using 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.*

When unescorted, 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 shall be directed to the designated entrance. Visitors entering the area shall 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 driver's license. When leaving the area, the entry control monitor or escort should enter the visitor's time of departure.

Each restricted area register will 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 posted at the front desk and vendors should be required to sign and the monitor should not be required to make an entry in the Restricted Area Register. If there is any doubt on the identity of the individual prior to permitting entry, the entry control clerk should verify the identity prior to permitting entry.

### *4.3.2 Controlling Physical Access to FTI*

Management or the designee shall maintain an authorized list of all personnel who have access to information system areas, where these systems contains FTI. This shall not apply to those areas within the facility officially designated as publicly accessible.

In addition, the site shall issue appropriate authorization credentials. In addition, a list shall be maintained that identifies those individuals who have authorized access to any systems where FTI is housed. Access authorizations and records maintained in electronic form are acceptable.

Designated officials or designee within the organization shall review and approve the access list and authorization credentials. The access list to the systems and areas processing FTI must be updated at least annually. (Exhibit 4, PE-2)

The entity shall control all access points to the facility. This shall not apply to areas officially designated as publicly accessible. The agency shall ensure that individual

access is authorized and verified before granting access to the facility. (Exhibit 4, PE-3)

Each agency shall control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. (Exhibit 4, PE-5).

The agency or designee shall monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. (Exhibit 4, PE-6)

A visitor access log shall be used to authenticate visitors before authorizing access to the facility where the information system resides and contains FTI. This does not apply to areas designated as publicly accessible. (Exhibit 4, PE-7)

The visitor access log shall contain the following information:

(i) name and organization of the visitor;

(ii) signature of the visitor;

(iii) form of identification;

(iv) date of access;

(v) time of entry and departure;

(vi) purpose of visit; and

(vii) name and organization of person visited.

Designated officials or designees within the organization review the visitor access records, at least annually. (Exhibit 4, PE-8)

For all IT systems that house FTI, the agency shall authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items. (Exhibit 4, PE-16)

For all areas that process FTI, the agency shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. (Exhibit 4, PE-18)

### *4.3.3 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 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.

Whenever cleaning and maintenance are performed and there is FTI that may be accessible, the cleaning and maintenance must be done in the presence of an authorized employee.

### *4.3.4 Secured Interior/Secured Perimeter*

Secured areas are internal areas that have been designed to prevent undetected entry by unauthorized persons during duty and non-duty hours. Non agency personnel may not reside in computer rooms and/or areas containing FTI unless the person is authorized to access that FTI. Secured perimeter/secured area must meet the following minimum standards:

- This area must be 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.

### *4.3.5 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 storing 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.

### *4.3.6 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. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

### *4.3.7 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.

### *4.3.8 Safes/Vaults*

A safe is a General Services Administration (GSA)-approved container of Class I, IV, or V, or Underwriters Laboratories Listing of TRTL-30, TRTL-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.

### *4.3.9 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 replacement when necessary. Accountability records will be maintained on keys and will include taking an inventory of total keys available and issuing keys.

### *4.3.10 Control and Safeguarding Keys & Combinations*

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing 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, 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 issuing keys. A periodic reconciliation should be done on all key records.

### *4.3.11 Locking Systems for Secured Areas*

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
- A dead bolt throw of one inch or longer
- Double cylinder design. Cylinders are to have five or more pin tumblers
- Hardened inserts or be made of steel if bolt is visible when locked.

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 persons with 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.

### *4.3.12 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 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 protect and account for all FTI properly. FTI 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. FTI 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*

Handling FTI 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 electronic 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. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof.

### *4.6 Physical Security of Computers, Electronic, and Removable Media*

Because of the vast amount of data computers and electronic media store and process, the physical security and control of computers and electronic 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. Removable media must be labeled as FTI 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.*

Electronic media and removable 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 electronic media be maintained for 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 employee's 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.

In all instances, the agency shall employ appropriate management, operational, and technical information system security controls at alternate work sites. (Exhibit 4, PE-17)

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

### *4.7.1 Equipment*

Only agency-owned computers, media, and software will be used to process, access, and store FTI. The agency must retain ownership and control, for all hardware, software, and telecommunications equipment connecting to public communication networks, where these are resident at all alternate work sites.

*All computers and mobile devices that contain FTI and are resident in an alternate work site must employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost and/or stolen. (OMB Memo M-16)*

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 also should 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.

### *4.7.2 Storing Data*

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

**Note:** Additional information on Remote Access can be found in Section 5.6.17.3, Transmitting Federal Tax Information.

### *4.7.3 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. Electronic media that are to be reused must have files overwritten or degaussed.

The agency will prepare a plan for the security of alternative work site. The agency should coordinate with the managing host system(s) and any networks, and maintain documentation on the test. Before implementation, the agency will certify that the security controls are adequate for security needs. Additionally, the agency will promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules should address brief absences while employees are 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.

The agency should conduct periodic inspections of alternative work sites 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*).

***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 accordance with 'Locking Systems for Secured Areas'. 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 Locked means an area that is locked after business hours with keys or combinations that are controlled.

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. The containers should have only two keys. Strict control of keys is mandatory. Examples are mini safes, metal lateral key lock files, and metal pull drawer cabinets with center/off center lock bars secured by padlocks.

**Protection Alternative Chart**

| | **Perimeter Type** | **Interior Area Type** | **Container Type** |
|---|---|---|---|
| **Alternate #1** | Secured | | Locked |
| **Alternate #2** | Locked | Secured | |
| **Alternate #3** | Locked | | Security |

### *5.1 General*

Agencies are required by IRC Section 6103(p)(4)(C) to restrict access to FTI only to persons whose duties or responsibilities require access (see Exhibit 3, *Sec. 6103(p)(4) Safeguards* and Exhibit 5*, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information*). To assist with this requirement, 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 access or 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 performing 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 avoid maintaining 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 also will 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 electronic 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.
- When technically possible, data files, data sets, shares, etc. must be overwritten 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.

In the case of a Data Warehouse, FTI can be commingled if the proper security controls are installed. This would require data monitoring software that can administer security down to databases, data profiles, data tables, or data columns and rows. The FTI within any of the above can be back-end labeled and tagged with an IRS identifier. The same would pertain to any reports generated from the Data Warehouse. An example would be a server with relational database security software. It can be administered down to any of the above levels and an end user without IRS access permission will not see the data.

See Exhibit 6, *Data Warehouse Concepts & Security Requirements*.

Examples of commingling include:

- 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 provides the address, the information will not be considered return information, as long as the source code is revised. Again, "provided" means using the individual's or third party's knowledge or records as the source of information.

### *5.4 Access to FTI 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 Section 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 about particular State employees entitled to access FTI, forward your inquiry to the

Disclosure Manager at the IRS 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 subdivisions, such as cities or counties, for any purpose, including tax administration. Likewise, State tax agencies may not furnish FTI to any other states, even where agreements have been made, informally or formally, for the reciprocal exchange of State tax information. Also, non-government 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 Section 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 which data exchange agreements exist. Agencies may be authorized to obtain 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 Section 6103(l)(7)) and child support enforcement (IRC Section 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 the 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 an electronic media format, including removable media, 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:

#### 5.5.1 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 electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS Safeguard Reviews.

#### *5.5.2 Contractor or Agency-Shared Facility for Tax Administration or Federal Debt Collection*

This method may be used only by an agency that processes FTI for tax administration or Federal debt collection purposes. The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 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.

### *5.5.3 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 Section 6103(l)(7)) or those to whom child support obligations are sought to established or enforced pursuant to the provisions of part D of title IV of the Social Security Act (IRC Section 6103(l)(6)), and the refund offset disclosures (IRC Section 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 releasing electronic 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*

This section includes significant enhancements to the computer security standards agencies should meet to adequately protect Federal tax information under their administrative control.

The revised computer security framework was primarily developed using applicable guidelines specified in National Institute of Standards & Technology (NIST) Special Publication (SP) 800-30 *Risk Management Guide for Information Technology Systems* and (NIST) Special Publication (SP) 800- 53 *Recommended Security Controls for Federal Information Systems*. Only applicable NIST SP 800-53 controls for a moderate impact level are included in this publication as a baseline. Applicability was determined by selecting controls required to protect the confidentiality and integrity of FTI.

All agency information systems used for processing, storing and transmitting Federal tax information must enforce the security provisions described in this section. Agency information systems include the equipment, facilities and people that collect, process, store, display, and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use.

Impact levels used in this document are described in the Federal Information Processing Standards (FIPS) *Standards for Security Categorizations of Federal Information and Information Systems*. NIST documents are available at: http://csrc.nist.gov/publications/nistpubs/index.html.

NIST categorizes computer security controls into three main types: 1) Management, 2) Operational, and 3) Technical.

Management security controls focus on managing organizational risk and information system security and devising sufficient countermeasures or safeguards for mitigating risk to acceptable levels. Management security control families include risk assessment, security planning, system and services acquisition, and risk assessment.

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational security controls require technical or specialized expertise and often rely on management and technical security controls. Operational

security control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.

Technical security controls focus on the security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

Exhibit 4, *NIST Moderate Risk Controls for Federal Information Systems*; Exhibit 8, *Password Management Guidelines*, and Exhibit 9, *System Audit Management Guidelines* contain information that is intended to clarify the technical controls of this document.

The following sections provide the security controls that relate to protecting the information system, relative to the managerial, operational, and technical controls. For ease of reference, these have been placed in alphabetical order.

### *5.6.1. Access Control*

Access control policy and procedures must be developed, documented, disseminated, and updated, as necessary, to facilitate implementing access control security controls. Security controls include account management, access enforcement, limiting access to those with a need-to-know, information-flow enforcement, separation of duties, least privilege, unsuccessful login attempts, system use notification, session locks, session termination, and remote access. Please see Exhibit 4, *Access Controls* for additional detail.

Agencies must manage information system user accounts, including establishing, activating, changing, reviewing, disabling, and removing user accounts. The information system must enforce assigned authorizations for controlling system access and the flow of information within the system and between interconnected systems. Management must supervise and review the activities of the users as this relates to information system access. (Exhibit 4, AC-13)

In addition, the agency must identify and document specific user actions that can be performed on the information system without identification or authentication. Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible web site for which no authentication is required. (Exhibit 4, AC-14)

Agencies must ensure the information system enforces separation of duties through assigned access authorizations. The information system must enforce the most restrictive access capabilities users need (or processes acting on behalf of users) to perform specified tasks.

The information system must limit the number of consecutive unsuccessful access attempts allowed in a specified period and automatically perform a specific function (e.g., account lockout, delayed logon) when the maximum number of attempts is exceeded. The information system must display an approved system usage notification before granting system access informing potential users that (i) the system contains U.S. Government information; (ii) users actions are monitored and audited; and (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties. Policy must be enforced so that a workstation and/or application are locked after a pre-defined period. This will ensure that unauthorized staff or staff without a need-to-know cannot access FTI.

The following paragraphs address access controls when the system is accessed remotely. Virtual Private Network (VPN) (or similar technology providing similar protection (e.g., end-to-end encryption))

should be used when remotely accessing the system.

The information system shall automatically terminate any remote session after fifteen minutes of inactivity, where these systems contain FTI. For instances of interactive and/or batch processing, compensating controls must be implemented. (Exhibit 4, AC-12)

Agencies must authorize, document, and monitor all remote access capabilities used on the system, where these systems containing FTI. (Exhibit 4, AC-17).

Agencies must develop policies for any allowed wireless access, where these systems contain FTI. (Exhibit 4, AC-18)

As part of the wireless access, the agency shall authorize, document, and monitor all wireless access to the information system. Guides to secure wireless access implementation for this control are contained in NIST SP 800-48 Revision 1 (Wireless Network Security for IEEE 802.11a/b/g and Bluetooth) and NIST SP 800-97 (Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i), at a minimum.

Agencies must develop policies for any allowed portable and mobile devices, where these systems contain FTI. (Exhibit 4, AC-19) As part of this, the agency shall authorize, document, and monitor all device access to organizational information systems.

Agencies must develop policies for authorized individuals to access the information systems from an external system, such as access allowed from an alternate work site. This policy shall address the authorizations allowed to transmit, store, and/or process FTI. As part of this, the agency shall authorize, document, and monitor all access to organizational information systems, where these systems contain FTI. (Exhibit 4, AC-20)

### *5.6.2 Audit & Accountability*

Audit and accountability policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing audit and accountability security controls. Such audit and accountability security controls include auditable events; content of audit records; audit storage capacity; audit processing; audit monitoring, analysis and reporting; time stamps; protecting audit information and audit retention.

The information system must generate audit records for all security-relevant events, including all security and system administrator accesses. An example of an audit activity is reviewing the administrator actions whenever security or system controls may be modified to ensure that all actions are authorized. Security-relevant events must enable the detection of unauthorized access to FTI data. System and/or security administrator processes will include all authentication processes to access the system, for both operating system and application-level events.

Audit logs must enable tracking activities taking place on the system. Exhibit 9, *System Audit Management Guidelines,* contains guidelines that can be used for creating audit-related processes.

The information system shall alert appropriate organizational officials in the event of an audit processing failure and takes the additional actions. (Exhibit 4, AU-5)

Agencies must configure the information system to allocate sufficient audit record storage capacity to record all necessary auditable items. At a minimum, the information system shall provide date and time stamps for use in audit record generation. (Exhibit 4, AU-8)

Agencies must routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials

for prompt resolution. To enable review of audit records, the information system provides an audit reduction and report generation capability. (Exhibit 4, AU-7)

To support the audit of activities, all agencies must ensure that audit information is archived for six years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.

The information system protects audit information and audit tools from unauthorized access, modification, and deletion. (Exhibit 4, AU-9)

### *5.6.3 Awareness & Training*

Awareness and training policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing awareness and training security controls. Such awareness and training security controls include security awareness and security training. Agencies must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to the system. Agencies must identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities and provide sufficient security training before authorizing access to the information system and FTI.

Agencies must document and monitor individual information system security training activities including basic security awareness training and specific information system security training. (Exhibit 4, AT-4)

### *5.6.4 Certification & Accreditation (C&A)*

The agency shall develop and update a policy that addresses the processes used to test, validate, and authorize the security controls used to protect FTI. While state and local agencies are not required to conduct a NIST compliant C&A, the agency shall accredit in writing that the security controls have been adequately implemented to protect FTI. The written accreditation constitutes the agency's acceptance of the security controls and associated risks. However for federal agencies that receive FTI, a NIST compliance C&A is required in accordance with FISMA. (Exhibit 4, CA-1)

The agency shall conduct an assessment of the security controls in the information system, periodically but at least annually, to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This assessment shall complement the certification process to ensure that periodically the controls are validated as being operational. (Exhibit 4, CA-2)

The agency shall authorize and document all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis. (Exhibit 4, CA-3)

The agency shall conduct a formal assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Exhibit 4, CA-4)

As recipients of FTI, the agency is responsible to develop and update a Plan of Action and Milestones (POA&M) that shall identify any deficiencies related to FTI processing. The POA&M shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during the review processes, either internal or external. The POAM shall address implementation of security controls to reduce or eliminate known vulnerabilities in the system. (Exhibit 4, CA-5)

Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security accreditation. All information regarding the accreditation shall be provided to the Office of Safeguards as part of the Safeguard Activity Report. (Exhibit 4, CA-6)

While the Safeguard Procedures Report shall identify the security controls, the authorization of the system must come from an agency official validating that the system is ready for operation. [Note: This control requirement does not apply to non-federal systems.]

All agencies shall periodically, at least annually, monitor the security controls within the information system hosting FTI to ensure that the controls are operating, as intended. (Exhibit 4, CA-7)

### *5.6.5 Configuration Management*

Configuration management policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing configuration management security controls. Such configuration management security controls include:

- The organization develops, documents, and maintains a current baseline configuration of the information system. (Exhibit 4,CM-2)
- Authorize, document, and control changes to the information system. (Exhibit 4, CM-3)
- Monitor changes to the information system conducting security impact analysis to determine the effects of the changes. (Exhibit 4, CM-4)
- Approve individual access privileges and enforces physical and logical access restrictions associated with changes to the information system and generates, retains, and reviews records reflecting all such changes. (Exhibit 4, CM-5)
- The agency shall establish mandatory configuration settings for information technology products employed within the information system, which (i) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (ii) documents the configuration settings; and (iii) enforces the configuration settings in all components of the information system. (Exhibit 4, CM-6)
- Restrict access for change, configuration settings, and provide the least functionality necessary
- Enforce access restrictions associated with changes to the information system
- Configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements (for additional guidance see NIST SP 800-70 *Security Configuration Checklists Program for IT Products- Guidance for Checklists Users and Developers*)
- Configure the information system to provide only essential capabilities
- Prohibit the use of functions, ports, protocols, and services not required to perform essential capabilities for processing, storing, or transmitting Federal tax information.
- Develop, document, and maintain a current inventory of the components of the information system and relevant ownership information. (Exhibit 4, CM-8)

### *5.6.6 Contingency Planning*

All FTI information that is transmitted to the states is backed up and protected within IRS facilities. As such, the controls of IT Contingency Planning are not required at the federal, state, or local agency. The primary contingency shall be to contact the IRS to obtain updated FTI data. If this timeframe extends beyond the IRS normal 60 day recovery period, agencies may not have immediate recovery of this information. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches.

If FTI is included in contingency planning; policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing contingency planning security controls.

In addition, plans must be periodically tested to ensure procedures and staff personnel are able to provide recovery capabilities within established timeframes. Such contingency planning security controls include alternate storage sites, alternate processing sites, telecommunications services, and information system and information backups. Agencies must identify alternate storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups. Agencies must identify alternate processing sites and/or telecommunications capabilities, and initiate necessary agreements to facilitate secure resumption of information systems used to process, store and transmit FTI if the primary processing site and/or primary telecommunications capabilities become unavailable. Agencies must conduct backups of user-level information, system-level information, and FTI and store such backups at a secure location.

### *5.6.7 Identification & Authentication*

Identification and authentication policy and procedures must be developed, documented, disseminated, and updated, as necessary, to facilitate implementing identification and authentication security controls. The information system must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics.

Agencies also must manage the user accounts assigned to the information system. Examples of effective user-account management practices include (i) obtaining authorization from appropriate officials to issue user accounts to intended individuals; (ii) disabling user accounts timely; (iii) archiving inactive or terminated user accounts; and (iv) developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by the information system.

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. (Exhibit 4, IA-6)

Whenever agencies are employing cryptographic modules, the agency shall work to ensure these modules are compliant with NIST guidance, including FIPS 140-2 compliance. (Exhibit 4, IA-7)

### *5.6.8 Incident Response and Incident Reporting*

Incident response policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate the implementing incident response security controls. Such incident response security controls include incident response training and incident reporting and monitoring.

Agencies must train personnel in their incident response roles on the information system and FTI. Incident response training must provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication, and recovery. Agencies must routinely track and document information system security incidents potentially affecting the confidentiality of FTI.

The agency shall test and/or exercise the incident response capability for the information system at least annually to determine the incident response effectiveness and documents the results. (Exhibit 4, IR-3)

Any time there is a compromise to FTI, the agency promptly reports incident information to the appropriate Agent-in-Charge, TIGTA. (Exhibit 4, IR-6)

The agency shall also provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability. (Exhibit 4, IR-7)

### *5.6.9 Maintenance*

Maintenance policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing maintenance security controls. Such maintenance security controls include identifying and monitoring a list of maintenance tools and remote maintenance tools. Agencies must approve, control, and routinely monitor the use of information system maintenance tools and remotely-executed maintenance and diagnostic activities. The agency allows only authorized personnel to perform maintenance on the information system. (Exhibit 4, MA-5)

The agency must ensure that maintenance is scheduled, performed, and documented. The agency must review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. (Exhibit 4, MA-2)

### *5.6.10 Media Access Protection*

Media access policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing media protection policy. Policies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls. (Exhibit 4, MP-1)

The agency shall restrict access to information system media to authorized individuals, where this media contains FTI. (Exhibit 4, MP-2)

The agency will physically control and securely store information system media within controlled areas, where this media contains FTI. (Exhibit 4, MP-4)

The agency must protect and control information system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

All media being transmitted from the IRS must employ the use of encryption. (Exhibit 4, MP-5)

The agency shall sanitize information system media prior to disposal or release for reuse. (Exhibit 4, MP-6)

### *5.6.11 Personnel Security*

Personnel security policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing personnel security controls. Such personnel security controls include position categorization, personnel

screening, personnel termination, personnel transfer, and access agreements.

Agencies must assign risk designations to all positions and establish screening criteria for individuals filling those positions. Individuals must be screened before authorizing access to information systems and information.

Agencies must terminate information system access, conduct exit interviews, and ensure return of all information system-related property when employment is terminated.

Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization. Appropriate access agreements must be completed before authorizing access to users requiring access to the information system and Federal Tax Information. Agencies must also establish a formal sanctions process for personnel who fail to comply with established information security policies, as this relates to FTI. Personnel security requirements must be established for third-party providers and monitored for provider compliance.

### *5.6.12 Planning*

Security planning policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing security planning controls. Such security planning controls include system security plans, system security plan updates and rules of behavior. Agencies must develop, document, and establish a system security plan (see Section 7.2, Safeguard Procedures Report) by describing the security requirements, current controls and planned controls, for protecting agency information systems and Federal tax information. The system security plan must be updated to account for significant changes (see Section 7.4, *Annual Safeguard Activity Report*) in the security requirements, current controls and planned controls for protecting agency information systems and Federal tax information. Agencies must develop, document, and establish a set of rules describing their responsibilities and expected behavior for information system use for users of the information system.

The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. (Exhibit 4, PL-6)

### *5.6.13 Risk Assessment*

Risk assessment policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing risk assessment controls. Such risk assessment controls include risk assessments and risk assessment updates. Agencies must conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of FTI (Exhibit 4, RA-3).

The agency must update the risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system (Exhibit 4, RA-4).

Periodically, systems that contain FTI shall be scanned to identify any vulnerabilities in the information system. The agency shall identify the timeframe on how often scans are conducted. (Exhibit 4, RA-5)

### *5.6.14 System & Services Acquisition*

System and services acquisition policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing system and services acquisition controls. Such system and services acquisition controls include information system documentation and outsourced information system services. Agencies must ensure that there is sufficient information system documentation, such as a Security Features Guide. Agencies must ensure third-party providers of information systems, who are used to process, store and transmit Federal tax information, employ security controls consistent with Safeguard computer security requirements.

The agency shall document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system. (Exhibit 4, SA-2)

Whenever information systems contain FTI, the agency manages the information system using a system development life cycle methodology that includes information security considerations. (Exhibit 4, SA-3)

Whenever information systems contain FTI, the agency shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk (Exhibit 4, SA-4)

Whenever information systems contain FTI, the agency shall obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system. (Exhibit 4, SA-5)

Whenever information systems contain FTI, the agency complies with software usage restrictions. (SA-6 SOFTWARE USAGE RESTRICTIONS)

Whenever information systems contain FTI, the agency shall enforce explicit rules governing the installation of software by users. (Exhibit 4, SA-7)

Whenever information systems contain FTI, the agency shall design and implement the information system using security engineering principles. (Exhibit 4, SA-8)

The information system developers shall create a security test and evaluation plan, implement the plan, and document the results. **(**Exhibit 4, SA-11)

### *5.6.15 System & Communications Protection*

System and communications policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing effective system and communications. (Exhibit 4, SC-1)

These controls shall include the following:

- procedures to remove residual data
- procedures to provide transmission confidentiality and to validate cryptography.

This reallocation of memory (storage) for reuse by the information system is known as object reuse. Information systems must be configured to prevent residual data from being shared with, recovered, or accessed by unauthorized users (or processes acting on behalf of users) once such data is removed from the information system and the memory once occupied by such data is reallocated to the information system for reuse, as applicable.

The information system shall separate front end interface from the back end processing and data storage. (Exhibit 4, SC-2)

The information system shall prevent unauthorized and unintended information transfer via shared system resources. (Exhibit 4, SC-4)

The information system shall be configured to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. (Exhibit 4, SC-7)

The information system must protect the confidentiality of FTI during electronic transmission. When cryptography (encryption) is employed within the information system, the system must perform all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation. Cryptographic data transmissions are ciphered and consequently unreadable until deciphered by the recipient.

Whenever there is a network connection, the information system shall terminate the network connection at the end of a session or after no more than fifteen minutes of inactivity. (Exhibit 4, SC-10)

When Public Key Infrastructure (PKI) is used, the agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. (Exhibit 4, SC-12)

The information system shall prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. Collaborative mechanisms include cameras and microphones that may be attached to the information system. Users must be notified if there are collaborative devices connected to the system. (Exhibit 4, SC-15)

The agency shall establish PKI policies and practices, as necessary. (Exhibit 4, SC-17)

The agency shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously. All mobile code must be authorized by the agency official. (Exhibit 4, SC-18)

The agency shall establish, document and control usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies. (Exhibit 4, SC-19)

The information system shall provide mechanisms to protect the authenticity of communications sessions. (Exhibit 4, SC-23)

### *5.6.16 System & Information Integrity*

System and information integrity policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing system and information integrity security controls. Such system and information integrity security controls include flaw remediation, intrusion detection tools and techniques, information input restrictions, and information output handling and retention.

The information system must implement protection against malicious code (e.g., viruses, worms, Trojan horses) that, to the extent possible, includes a capability for automatic updates. Intrusion detection tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of the information system and FTI.

Agencies must restrict information system input to authorized personnel (or processes acting on behalf of such personnel) responsible for processing, storing, or transmitting FTI.

Agencies must identify, report, and correct information system flaws. (Exhibit 4, SI-2)

The agency shall receive and review information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. (Exhibit 4, SI-5)

Agencies must handle and retain output from the information system, as necessary to document that specific actions have been taken. (Exhibit 4, SI-12).

### *5.6.17 Additional Computer Security Controls*

#### *5.6.17.1 Data Warehouse*

The concept of data warehousing consists of a collection of multi-dimensional integrated databases that are used to provide accessible information to clients or end users. The data can be manipulated through different categories or dimensions to facilitate analyzing data in relational databases. The result can provide the client or end user with an enterprise view or snapshot of the information.

Security requirements apply to data warehousing environments, as well as to typical networked environments.

Exhibit 6, *Data Warehouse Concepts & Security Requirements*, provides those unique requirements for this environment.

#### *5.6.17.2 Transmitting FTI*

All FTI data in transit must be encrypted, when moving across a Wide Area Network (WAN).

Generally, FTI transmitted within the Local Area Network (LAN) should be encrypted. If encryption is not used, the agency must use other compensating mechanisms (e.g., switched vLAN technology, fiber optic medium, etc.) to ensure that FTI is not accessible to unauthorized users.

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).

In instances where encryption is not used, the agency must ensure that all wiring, conduits, and cabling are within the control of agency personnel and that access to routers and network monitors are strictly controlled.

#### *5.6.17.3 Remote Access*

Accessing databases containing FTI from a remote location, i.e., a location not directly connected to the Local Area Network (LAN), will require adequate safeguards to prevent unauthorized entry. The IRS policy for allowing access to systems containing 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 a special (encrypted) modem and/or Virtual Private Network (VPN) for every workstation and a smart card (microprocessor) for every user. Smart cards should have both identification and authentication features and should provide data encryption as well. Two-factor authentication is recommended whenever FTI is being accessed from an alternate work location.

#### *5.6.17.4 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*).

### *5.6.17.5 Electronic Mail*

Generally, FTI shall not be transmitted or used on E-mail systems. If necessary, the following precautions must be taken to protect FTI sent via E-mail:

- Do not send FTI unencrypted in any email messages
- 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.

### *5.6.17.6 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.
- 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.

### *6.1 General*

IRC Section 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 and least expensive method agencies can use to protect sensitive information.

### *6.2 Employee Awareness*

Granting agency employee 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 Sections 7431, 7213(a), and 7213A (see Exhibit 5, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 10, *IRC Sec. 7213 Unauthorized Disclosure of Information*).

**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 unauthorized access "UNAX" violations, address, and hotline number)
- Use warning banners during initial logon on computers housing FTI
- Send e-mail and other electronic messages to inform users.

### *6.3 Internal Inspections*

Another measure IRS requires 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 the IRC and the IRS impose. 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 18-month cycle.

These requirements are discussed in greater detail throughout this publication. Key areas that should be addressed include:

### *6.3.1 Record Keeping*

Each agency, and functions within that agency, shall maintain a log of all requests for return information, including receipt and/or disposal of returns or return information. Return information will include any medium containing FTI, such as computer tapes, cartridges, or compact disks (CDs), or data received electronically. Receipt of information shall include all information received either directly or indirectly.

### *6.3.2 Secure Storage*

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

### *6.3.3 Limited Access*

Access to returns and return information (including tapes, cartridges, or other removable media) 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. An assessment of facility security features should be included in the report.

### *6.3.4 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*.

### *6.3.5 Computer Systems Security*

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

- Access to FTI is limited to those personnel who have a need-to-know. This need-to-know must be enforced electronically as well as physically. *(See Section 5.6, Computer Security)*.

**Note:** The review of the computer facility also should include the evaluation of computer security and physical security controls.

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.

**Note:** Exhibits 11, *Encryption Standards* and Exhibit 12, *Glossary* have been included in this document to clarify the terms and concepts used within.

### *7.1 General*

IRC Section 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 shall 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 Section 6103(p)(4) and the agency's own security requirements.

**Note:** Agencies must submit a new SPR whenever significant changes occur in their safeguard program or every six (6) years. Significant changes would include, but are not limited to, new computer equipment, facilities, or systems.

### *7.2 Safeguard Procedures Report*

Agencies shall submit their SPR on the template developed by the Office of Safeguards. The most current template may be requested by contacting SafeguardReports@irs.gov .

The SPR shall be accompanied by a letter on the agency's letterhead signed by the head of the agency or delegate. Information requested on the template includes:

#### *7.2.1 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 implementing the safeguard procedures.

#### *7.2.2 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 FTI is processed by the agency; it states how it is protected from unauthorized disclosure by that agency.*

#### *7.2.3 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 provide accurate accounting.

#### *7.2.4 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 or other

removable media). 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.

### *7.2.5 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.

### *7.2.6 Restricting Access to the Data*

A description of the procedures or safeguards 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.

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

### *7.2.7 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 that the records were destroyed (See 7.2.4 above.)

### *7.2.8 Information Technology (IT) Security*

A description of all automated information systems and networks that receive, process, store, or transmit FTI. These systems must have safeguard measures in place to restrict access to sensitive data (see Section 5.6). These safeguards should address all key components of IT security.

They should:

- 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 the destruction of the data.
- Have additional comments regarding the safeguards employed to ensure the protection of the computer.
- Describe in detail the security precautions undertaken if the agency's computer systems are connected or planned to be connected to other systems.

The Safeguard Procedures Report must include procedures for ensuring that all data is safeguarded from unauthorized access or disclosure.

### *7.2.9 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 Submitting Safeguard Procedures Report*

Federal, Child Support Enforcement, State Welfare agencies, Revenue Agencies, and

Local Taxing Authorities requesting FTI should submit their report electronically to:

SafeguardReports@irs.gov

**NOTE:** Reports should be sent electronically and encrypted via IRS approved encryption techniques. Paper submissions will no longer be accepted.

### *7.4 Annual Safeguard Activity Report*

Agencies shall submit their SAR on the template developed by the Office of Safeguards. The most current template may be requested by contacting SafeguardReports@irs.gov.

The SAR should be accompanied by a letter on the agency's letterhead signed by the head of the agency or delegate, dated.

#### *7.4.1 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

#### *7.4.2 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, including copies of destruction logs.

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

D. Other information to support the protection of FTI, in accordance with IRC 6103 (p)(4) requirements.

#### *7.4.3 Actions on Safeguard Review Recommendations*

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

#### *7.4.4 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.

### *7.4.5 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*

Agencies must submit their reports to the Office of Safeguards electronically. Reports must be sent encrypted via IRS approved encryption techniques. The email address for all reports is:

SafeguardReports@irs.gov.

**Federal Agencies** should submit their reports for the calendar year by January 31 of the following year.

**Law Enforcement Agencies** receiving Form 8300, under IRC Section 6103(l)(15), information should submit their reports for the processing year (May 1 through April 30) by June 30.

**Other State Agencies** (i.e., Departments of Labor, Departments of Transportation, etc.) receiving FTI under IRC 6103(d) and agencies receiving FTI under IRC 6104(c) with charitable organization oversight should submit their reports for the processing year by (June 1 through May 31) by June 30.

**State Tax Agencies** should submit their reports for the calendar year by January 31 of the following year.

**State Welfare Agencies and the DC Retirement Board** should submit their reports for the processing year (September 1 through August 31) by September 30.

**State Child Support Enforcement Agencies** should submit their reports for the calendar year by (March 31 through February 28) by March 31.

**Note:** Educational institutions receiving FTI under IRC Section 6103(m)(4)(B) should send reports to the oversight agency.

## DISPOSING FEDERAL TAX INFORMATION IRC 6103(p)(4)(F) SECTION 8.0

### *8.1 General*

Users of FTI are required by IRC Section 6103(p)(4)(F) to take certain actions after using Federal tax information to protect its confidentiality (see Exhibit 3, *Sec 6103(p)(4) Safeguards, and Exhibit 5, IRC Sec. 7431 Civil Damages for Unauthorized Disclosures of Returns and Return Information*). Agency officials and employees either will 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 and microfiche should be shredded to effect a 1/35- inch by 3/8- inch strips. If shredding is part of the overall destruction of FTI, strips can in effect be set at the industry standard (currently ½"). However, when deviating from IRS' 5/16" requirement, FTI 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 of data should be accomplished only after material has been shredded.

**Note**: NIST SP 800-088, Guidelines for Media Sanitization, contains supplemental information for media disposal.

### *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 Treasury Regulations (CTR) 301.6103(n)-1. The required safeguard language is contained in Exhibit 7, *Contract Language for General Services*. 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 Section 6103 authorizes the disclosure of FTI for use in statistical reports, for tax administration purposes, and certain other purposes specified in IRC Section 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 seeking statistical information from IRS should make their requests under IRC 6103(j). The requests should be addressed to:

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

## REPORTING IMPROPER INSPECTIONS OR DISCLOSURES SECTION 10.0

### *10.1 General*

Upon discovering a possible improper inspection or disclosure of FTI, including breeches and security incidents, 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 (TIGTA).

| Field Division | States Served by Field Division | Telephone Number |
|---|---|---|
| Atlanta | Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee | (404) 338-7449 |
| Chicago | Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, Ohio, North Dakota, South Dakota, Wisconsin | (312) 886-0620 |
| Dallas | Arkansas, Kansas, Louisiana, Mississippi, Missouri, Nebraska, Oklahoma, Texas | (972) 308-1400 |
| Denver | Alaska, Arizona, Colorado, Idaho, Montana, New Mexico, Nevada, Oregon, Utah, Washington, Wyoming | (303) 446-1880 |
| New York | Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, Vermont | (917) 408-5641 |
| San Francisco | California, Hawaii | (510) 637-2558 |
| Washington | Delaware, Maryland, New Jersey, Pennsylvania, Virginia, Washington DC, West Virginia | (202) 283-3001 |
| 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**

**Web Site:** **www.treas.gov/tigta**

### *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 encouraged 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, the agency should take certain precautions 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 7, *Contract Language for General Services).*

Agencies should fully report to the IRS all disclosures of FTI to contractors in their SPR. Additional disclosures to contractors should be reported on the annual SAR.

Engaging a contractor who may have incidental or inadvertent access to FTI does not come under these requirements. Only those contractors whose work will involve disclosing FTI in performing their duties are required to address these issues.

### *11.3 State Tax Officials and State and Local Law Enforcement Agencies IRC Section 6103(d)*

State taxing authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, administering State tax laws. However, the IRS, pursuant to Treasury Regulation 301.6103(n)-1, requires that agencies notify the IRS prior to executing 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 Section 6103(l)(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 1998 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 IRC Section 6402(c) in any overpayment otherwise payable to such individual.

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

### *11.5 Federal, State, and Local Welfare Agencies IRC Section 6103(l)(7)*

No officer or employee of any Federal, State, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of FTI.

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

### *11.6 Deficit Reduction Agencies IRC Section 6103(l)(10)*

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

### *11.7 The Center for Medicare and Medicaid Services IRC Section 6103(l)(12)(C)*

The Center for Medicare and Medicaid Services (CMS) is authorized under IRC Section 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 contractual relationship must exist between CMS and the agent. The agent, however, is not authorized to make further disclosures of IRS information.

### *11.8 Disclosures Under IRC Section 6103(m)(2)*

Disclosures to agents of a Federal agency under IRC Section 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

**FEDERAL REGISTER:**

**PROCEDURES FOR ADMINISTRATIVE REVIEW OF A DETERMINATION THAT AN AUTHORIZED RECIPIENT HAS FAILED TO SAFEGUARD TAX RETURNS OR RETURN INFORMATION AND PROCEDURES FOR ADMINISTRATIVE REVIEW OF A DETERMINATION THAT AN AUTHORIZED RECIPIENT HAS FAILED TO SAFEGUARD TAX RETURNS OR RETURN INFORMATION**

**Federal Register** / Vol. 71, No. 37 / Friday, February 24, 2006 / Proposed Rules **9487**

**DEPARTMENT OF THE TREASURY**

**Internal Revenue Service**

**26 CFR Part 301**

**[REG–157271–05]**

**RIN 1545–BF21**

**Procedures for Administrative Review of a Determination That an Authorized Recipient Has Failed To Safeguard Tax Returns or Return Information**

**AGENCY:** Internal Revenue Service (IRS), Treasury.

**ACTION:** Notice of proposed rulemaking by cross-reference to temporary regulations.

**SUMMARY:** In the Rules and Regulations section of this issue of the **Federal Register**, the IRS is issuing temporary regulations regarding administrative review procedures for certain government agencies and other authorized recipients of tax returns or return information (authorized recipients) whose receipt of returns and return information may be suspended or terminated because they do not maintain proper safeguards. The temporary regulations provide guidance to responsible IRS personnel and authorized recipients as to these administrative procedures. The text of the temporary regulations published in the Rules and Regulation section of this issue of the **Federal Register** serves as the text of the proposed regulations.

**DATES:** Written and electronic comments and requests for a public hearing must be received by May 25, 2006.

**ADDRESSES:** Send submissions to: CC:PA:LPD:PR (REG–157271–05), Room 5203, Internal Revenue Service, P.O. Box 7604, Ben Franklin Station, Washington, DC 20044. Submissions may be hand-delivered between the hours of 8 a.m. and 4 p.m. to CC:PA:LPD:PR (REG–157271–05), Courier's Desk, Internal Revenue Service, 1111 Constitution Avenue, NW., Washington, DC, or sent electronically, via the IRS Internet site at *http://www.irs.gov/regs,* or via the Federal eRulemaking Portal at *http://www.regulations.gov* (IRS and REG–148864–03).

**FOR FURTHER INFORMATION CONTACT:**
Concerning submission of comments, Treena Garrett, (202) 622–7180; concerning the temporary regulations, Melinda K. Fisher, (202) 622–4580 (not toll-free numbers).

**SUPPLEMENTARY INFORMATION:**

**Background**

Under section 6103 of the Internal Revenue Code (Code), tax returns and return information are protected from disclosure except in specifically enumerated circumstances. Where disclosure is permitted, section 6103 generally imposes strict safeguarding requirements and requires the IRS to monitor and enforce compliance with those requirements. Section 6103(p)(7) requires the Secretary of the Treasury to prescribe procedures providing for administrative review of any determination under section 6103(p)(4) that an agency, body, or commission receiving returns or return information pursuant to section 6103(d) has failed to meet the safeguarding requirements. Withdrawn § 301.6103(p)(7)–1 set forth the procedures for terminating future disclosures to these authorized recipients. These proposed regulations provide the intermediate review and termination procedures for all authorized recipients identified in section 6103(p)(4).

With an increasing volume of authorized disclosures of returns and return information, it is critical that authorized recipients of returns and return information adhere to the strict safeguard requirements of the Code and that the IRS take all necessary steps to ensure that those requirements are met. If unauthorized disclosures do occur, it is similarly important that the IRS take steps to address them and ensure that they are not repeated. Such steps include, as appropriate, suspension or termination of further disclosures to an authorized recipient. Nevertheless, because the authority to receive returns and return information is provided by law, authorized disclosures should not be suspended or terminated for failure to maintain adequate safeguards without appropriate administrative review procedures. The temporary regulations set forth procedures to ensure that authorized recipients provide the proper security and protection to returns and return information.

Temporary regulations in the Rules and Regulations section of this issue of the **Federal Register** amend the Procedure and Administration Regulations (26 CFR part 301) relating to section 6103(p)(4) and (p)(7). The temporary regulations provide the intermediate review and termination procedures for all authorized recipients. The text of the temporary regulations also serves as the text of these proposed regulations. The preamble to the temporary regulations explains the proposed regulations.

**Special Analyses**

It has been determined that this notice of proposed rulemaking is not a significant regulatory action as defined in Executive Order 12866. Therefore, a regulatory assessment is not required. Pursuant to the Regulatory Flexibility Act (5 U.S.C. chapter 6), it is hereby certified that these regulations will not have a significant economic impact on a substantial number of small businesses. These regulations do not impose burdens or obligations on any person, but instead provide certain rights of administrative review. Accordingly, a regulatory flexibility analysis is not required. Pursuant to

section 7805(f) of the Code, these proposed regulations will be submitted to the Chief Counsel for Advocacy of the Small Business Administration for comment on their impact on small business.

**Comments and Requests for a Public Hearing**

Before these proposed regulations are adopted as final regulations, consideration will be given to any electronic and written comments (a signed original and eight (8) copies) that are submitted timely to the IRS. The IRS and Treasury Department specifically request comments on the clarity of the proposed regulations and how they can be made easier to understand. All comments will be available for public inspection and copying. A public hearing may be scheduled if requested in writing by a person who timely submits comments. If a public hearing is scheduled, notice of the date, time, and place for the hearing will be published in the **Federal Register**.

**Drafting Information**

The principal author of these regulations is Melinda K. Fisher, Office of the Associate Chief Counsel (Procedure & Administration), Disclosure and Privacy Law Division.

**List of Subjects in 26 CFR Part 301**

Employment taxes, Estate taxes, Excise taxes, Gift taxes, Income taxes, Penalties, Reporting and recordkeeping requirements.

**Proposed Amendments to the Regulations**

Accordingly, 26 CFR part 301 is proposed to be amended as follows:

**PART 301—PROCEDURE AND ADMINISTRATION**

**Paragraph 1.** The authority citation for part 301 is amended, in part, by adding an entry in numerical order to read as follows:

**Authority:** 26 U.S.C. 7805 * * * Sections 301.6103(p)(4)–1 and 301.6103(p)(7)–1 also issued under 26 U.S.C. 6103(p)(4) and (7) and (q); * * *

**Par. 2.** Section 301.6103(p)(4)–1 is added to read as follows:

**§ 301.6103(p)(4)–1 Procedures relating to safeguards for returns or return information.**

[The text of proposed § 301.6103(p)(4)–1 is the same as the text of § 301.6103(p)(4)–1T published elsewhere in this issue of the **Federal Register**].

**Par. 3.** Section 301.6103(p)(7)–1 is added to read as follows:

**§ 301.6103(p)(7)–1 Procedures for administrative review of a determination that an authorized recipient has failed to safeguard tax returns or return information.**

[The text of proposed § 301.6103(p)(7)–1 is the same as the text of § 301.6103(p)(7)–1T published elsewhere in this issue of the **Federal Register**].

**Mark E. Matthews,**
*Deputy Commissioner for Services and Enforcement.*
[FR Doc. 06–1714 Filed 2–23–06; 8:45 am]
BILLING CODE 4830–01–U

---



**DEPARTMENT OF THE TREASURY**

**Internal Revenue Service**

**26 CFR Part 301**

**[TD 9252]**

**RIN 1545–BF22**

**Procedures for Administrative Review of a Determination That an Authorized Recipient Has Failed to Safeguard Tax Returns or Return Information**

**AGENCY:** Internal Revenue Service (IRS), Treasury.

**ACTIONS:** Temporary regulations.

**SUMMARY:** This document contains temporary regulations regarding administrative review procedures for certain government agencies and other authorized recipients of tax returns or return information (authorized recipients) whose receipt of returns and return information may be suspended or terminated because they do not maintain proper safeguards. The temporary regulations provide guidance to responsible IRS personnel and authorized recipients as to these administrative procedures. The text of these temporary regulations serves as the text of the proposed regulations set forth in the notice of proposed rulemaking on this subject in the Proposed Rules section of this issue of the **Federal Register**.

**DATES:** *Effective Date:* These regulations are effective February 24, 2006.
*Applicability Date:* For dates of applicability, see § 301.6103(p)(7)–1T(e).

**FOR FURTHER INFORMATION CONTACT:**
Melinda Fisher, (202) 622–4580 (not a toll-free number).

**SUPPLEMENTARY INFORMATION:**

**Background**

Under section 6103 of the Internal Revenue Code (Code), tax returns and return information are protected from disclosure except in specifically enumerated circumstances. Where disclosure is permitted, section 6103 generally imposes strict safeguarding requirements and requires the IRS to monitor and enforce compliance with those requirements. Section 6103(p)(7) requires the Secretary of the Treasury to prescribe procedures providing for administrative review of any determination under section 6103(p)(4) that an agency, body, or commission receiving returns or return information pursuant to section 6103(d) has failed to meet the safeguarding requirements. Withdrawn § 301.6103(p)(7)–1 set forth the procedures for terminating future disclosures to these authorized recipients. These temporary regulations provide the intermediate review and termination procedures for all authorized recipients identified in section 6103(p)(4).

With an increasing volume of authorized disclosures of returns and

return information, it is critical that authorized recipients of returns and return information adhere to the strict safeguard requirements of the Code and that the IRS take all necessary steps to ensure that those requirements are met. If unauthorized disclosures do occur, it is similarly important that the IRS take steps to address them and ensure that they are not repeated. Such steps include, as appropriate, suspension or termination of further disclosures to an authorized recipient. Nevertheless, because the authority to receive returns and return information is provided by law, authorized disclosures should not be suspended or terminated without appropriate administrative review procedures. These temporary regulations set forth procedures to ensure that authorized recipients provide the proper security and protection to returns and return information.

**Explanation of Provisions**

There are four basic parts to the statutory scheme Congress created in section 6103 of the Code to protect the confidentiality of tax returns and return information:

1. The general rule that makes returns and return information confidential except as expressly authorized in the Code;

2. The exceptions to the general rule detailing permissible disclosures;

3. Technical, administrative, and physical safeguard provisions to prevent authorized recipients of returns and return information from inspecting, using, or disclosing the returns and return information in an unauthorized manner, and accounting, recordkeeping and reporting requirements that detail what inspections and disclosures are made for certain purposes to assist in oversight; and

4. Criminal penalties for the willful unauthorized inspection or disclosure of returns and return information and a civil cause of action for the taxpayer whose returns or return information has been inspected or disclosed in a manner not authorized by the Code.

Section 6103(p)(4) provides that no returns or return information may be disclosed by the IRS to certain government agencies and other authorized recipients unless they establish procedures satisfactory to the IRS for safeguarding the returns and return information they receive. These procedures are set forth in Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, which is available at *http://www.irs.gov/formspubs/list.* Disclosure of returns and return information to the authorized recipients described in section 6103(p)(4) is conditioned on the recipient maintaining a secure place for storing the returns and return information, restricting access to returns and return information to persons whose duty requires access and to whom disclosure can be made under the internal revenue laws, providing other safeguards necessary to keeping the returns and return information confidential, reporting to the IRS on the safeguard procedures, and returning to the IRS or destroying the returns and return information upon completion of use. The IRS reviews, on a regular basis, safeguards established by authorized recipients of returns and return information.

If there are any unauthorized inspections or disclosures of returns or return information by authorized recipients, further disclosures may be terminated or suspended until the IRS is satisfied that adequate protective measures have been taken to prevent a recurrence of unauthorized inspection or disclosure. In addition, the IRS may terminate or suspend disclosure to any authorized recipient if the IRS determines that adequate safeguards are not being maintained.

The Code, in section 6103(p)(4), (p)(7), and (q) authorizes the IRS to promulgate regulations to carry out its statutory safeguard responsibilities. More specifically, section 6103(p)(7) requires that the IRS promulgate regulations establishing procedures for an administrative review of any determination by the IRS under section 6103(p)(4) that a State tax agency authorized to receive returns and return information under section 6103(d) has failed to meet the requirements of section 6103(p)(4). See Tax Reform Act of 1976, S. Rep. 94–938, 94th Cong., 2d Sess. 345 (1976). Under current § 301.6103(p)(7)–1 of the Procedure and Administration Regulations (26 CFR Part 301), the IRS has established procedures whereby State tax agencies that receive returns and return information pursuant to section 6103(d) have an opportunity, prior to a suspension or termination of disclosure, to contest a preliminary finding by the IRS of inadequate safeguards or unauthorized disclosure, or to establish that a State tax agency has taken steps to prevent a recurrence of the violation. This document adopts temporary regulations that extend the administrative review procedure applicable to State tax agencies to any authorized recipient specified in section 6103(p)(4) with respect to which the IRS has made a preliminary finding of inadequate safeguards or unauthorized disclosure. The temporary regulations also apply this administrative review procedure to any such authorized recipient with respect to which the IRS has made a preliminary finding as to unauthorized inspection of returns or return information. The temporary regulations treat unauthorized inspection in the same manner as unauthorized disclosure because both unauthorized acts are proscribed by the Code. In particular, section 7213A, enacted by the Taxpayer Browsing Protection Act of 1997, Public Law 105–35 (111 Stat. 1104), specifically treats the unauthorized inspection of a return or return information as a misdemeanor.

**Special Analyses**

It has been determined that these temporary regulations are not a significant regulatory action as defined in Executive Order 12866. Therefore, a regulatory assessment is not required. Pursuant to 5 U.S.C. 553(b)(B) it has been determined that prior notice and public comment on these temporary regulations are unnecessary and contrary to the public interest. These regulations do not impose any burdens or obligations on any person, but instead provide certain rights of administrative review. Moreover, these regulations are necessary to protect taxpayer confidentiality and the integrity of return information. For the same reasons, it has been determined pursuant to 5 U.S.C. 553(d)(3) that good cause exists to dispense with a delayed effective date for these regulations. For

applicability of the Regulatory Flexibility Act (5 U.S.C. chapter 6), please refer to the cross-reference notice of proposed rulemaking published elsewhere in this issue of the **Federal Register**. Pursuant to section 7805(f) of the Code, these temporary regulations will be submitted to the Chief Counsel for Advocacy of the Small Business Administration for comment on their impact on small business.

**Drafting Information**

The principal author of these temporary regulations is Melinda K. Fisher, Office of the Associate Chief Counsel (Procedure & Administration), Disclosure and Privacy Law Division.

**List of Subjects in 26 CFR Part 301**

Employment taxes, Estate taxes, Excise taxes, Gift taxes, Income taxes, Penalties, Reporting and recordkeeping requirements.

**Amendments to the Regulations**

Accordingly, 26 CFR Part 301 is amended as follows:

**PART 301—PROCEDURE AND ADMINISTRATION**

**Paragraph 1.** The authority citation for part 301 is amended by adding an entry in numerical order to read, in part, as follows:

**Authority:** 26 U.S.C. 7805 * * * Sections 301.6103(p)(4)–1 and 301.6103(p)(7)–1T also issued under 26 U.S.C. 6103(p)(4) and (7) and (q), * * *

**Par. 2.** Section 301.6103(p)(4)–1T is added to read as follows:

**§ 301.6103(p)(4)–1T Procedures relating to safeguards for returns or return information (temporary).**

For security guidelines and other safeguards for protecting returns and return information, see guidance published by the Internal Revenue Service. For procedures for administrative review of a determination that an authorized recipient has failed to safeguard returns or return information, see § 301.6103(p)(7)–1T.

**§ 301.6103(p)(7)–1 [Removed]**

**Par. 3.** Section 301.6103(p)(7)–1 is removed.

**Par. 4.** Section 301.6103(p)(7)–1T is added to read as follows:

**§ 301.6103(p)(7)–1T Procedures for administrative review of a determination that an authorized recipient has failed to safeguard returns or return information (temporary).**

(a) *In general.* Notwithstanding any section of the Internal Revenue Code, the Internal Revenue Service (IRS) may terminate or suspend disclosure of returns and return information to any authorized recipient specified in subsection (p)(4) of section 6103, if the IRS makes a determination that:

(1) The authorized recipient has allowed an unauthorized inspection or disclosure of returns or return information and that the authorized recipient has not taken adequate corrective action to prevent the recurrence of an unauthorized inspection or disclosure, or

(2) The authorized recipient does not satisfactorily maintain the safeguards prescribed by section 6103(p)(4), and has made no adequate plan to improve its system to maintain the safeguards satisfactorily.

(b) *Notice of IRS's intention to terminate or suspend disclosure.* Prior to terminating or suspending authorized disclosures, the IRS will notify the authorized recipient in writing of the IRS's preliminary determination and of the IRS's intention to discontinue disclosure of returns and return information to the authorized recipient. Upon so notifying the authorized recipient, the IRS, if it determines that tax administration otherwise would be seriously impaired, may suspend further disclosures of returns and return information to the authorized recipient pending a final determination by the Commissioner or a Deputy Commissioner described in paragraph (d)(2) of this section.

(c) *Authorized recipient's right to appeal.* An authorized recipient shall have 30 days from the date of receipt of a notice described in paragraph (b) of this section to appeal the preliminary determination described in paragraph (b) of this section. The appeal shall be made directly to the Commissioner.

(d) *Procedures for administrative review.* (1) To appeal a preliminary determination described in paragraph (b) of this section, the authorized recipient shall send a written request for a conference to: Commissioner of Internal Revenue (Attention: SE:S:CLD:GLD), 1111 Constitution Avenue, NW., Washington, DC 20224. The request must include a complete description of the authorized recipient's present system of safeguarding returns or return information, as well as a complete description of its practices with respect to the inspection, disclosure, and use of the returns or return information it (including any authorized contractors or agents) receives under the Internal Revenue Code. The request then must state the reason or reasons the authorized recipient believes that such system, or practice, including improvements, if any, to such system or practice expected to be made in the near future, is or will be adequate to safeguard returns or return information.

(2) Within 45 days of the receipt of the request made in accordance with the provisions of paragraph (d)(1) of this section, the Commissioner or Deputy Commissioner personally will hold a conference with representatives of the authorized recipient, after which the Commissioner or Deputy Commissioner will make a final determination with respect to the appeal.

(e) *Effective date.* This section is applicable to all authorized recipients of returns and return information that are subject to the safeguard requirements set forth in section 6103(p)(4) on or after February 23, 2006.

**Mark E. Matthews,**
*Deputy Commissioner for Services and Enforcement.*
Approved: February 11, 2006.

**Eric Solomon,**
*Acting Deputy Assistant Secretary of the Treasury (Tax Policy).*
[FR Doc. 06–1713 Filed 2–23–06; 8:45 am]
**BILLING CODE 4830–01–U**

**EXHIBIT 2**

# 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 law enforcement agency receiving information under subsection (i)(7)(A), any local child support enforcement agency, or any local agency administering a program listed in subsection (l)(7)(D) who has or had access to returns or return information under this section, and
(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (6), (12), (16), (19), or (20) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n),
shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes of 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 thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so 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, overassessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,
(B) any part of any written determination or any background file document relating to such written determination (as such terms are defined in section 6110 (b)) which is not open to public inspection under section 6110,
(C) any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to such agreement or any application for an advance pricing agreement, and
(D) any agreement under section 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement,
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 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 or related statutes (or equivalent laws and statutes of a State) and tax conventions to which the United States is 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 assessment, 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 subsections (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
(11) Terrorist incident, threat, or activity: The term “terrorist incident, threat, or activity” means an incident, threat, or activity involving an act of domestic terrorism (as defined in section 2331 (5) of title 18, United States Code) or international terrorism (as defined in section 2331(1) of such title).

**EXHIBIT 3**

# SEC. 6103(p)(4) SAFEGUARDS

Any Federal agency described in subsection (h)(2), (h)(5), (i)(1), (2), (3), (5), or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (13), (14), or (17), or (o)(1), the General Accounting Office, the Congressional Budget Office, or any agency, body, or commission described in subsection (d), (i)(3)(B)(i) or (7)(A)(ii), or (l)(6), (7), (8), (9), (12), (15), or (16) or any other person described in subsection (l)(16), (17), (19), or (20) 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 or 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, the General Accounting Office, or the Congressional Budget 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 (l)(6), (7), (8), (9), or (16), or any other person described in subsection (l)(16), (17), (19), or (20) 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 subsections [5] (h)(2), (h)(5), (i)(1), (2), (3), (5) or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (12), (13), (14), (15), or (17), or (o)(1),,[6] the General Accounting Office, or the Congressional Budget Office, either—

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

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

(III) 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 the conditions of subparagraphs (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 proceeding 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), (17), (19), or (20), or the General Accounting Office or the Congressional Budget Office has failed to, or does not, meet the 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), (17), (19), or (20), or the General Accounting Office or the Congressional Budget 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 (l) 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 1141(h)(2) of the Social Security Act).

**Exhibit 4**

***NIST Moderate Risk Controls for Federal Information Systems***

*Note: Missing or asterisked controls are not required for Publication 1075 compliance.*

SECURITY CONTROLS AND ENHANCEMENTS: MODERATE-IMPACT INFORMATION SYSTEMS

FAMILY: ACCESS CONTROL CLASS: TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually].

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [Assignment: organization-defined time period] of inactivity.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

AC-17 REMOTE ACCESS

Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.

FAMILY: AWARENESS AND TRAINING CLASS: OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

FAMILY: AUDIT AND ACCOUNTABILITY CLASS: TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [Assignment: organization-defined auditable events].

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment:

organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY CLASS: MANAGEMENT

ASSESSMENTS

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

FAMILY: CONFIGURATION MANAGEMENT CLASS: OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains a current baseline configuration of the information system.

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization authorizes, documents, and controls changes to the information system.

CM-4 MONITORING CONFIGURATION CHANGES

Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.

CM-6 CONFIGURATION SETTINGS

Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

FAMILY: CONTINGENCY PLANNING CLASS: OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

CP-2 CONTINGENCY PLAN

Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

*CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

CP-6 ALTERNATE STORAGE SITE

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

CP-7 ALTERNATE PROCESSING SITE

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.

*CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.

*CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.

*CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

FAMILY: IDENTIFICATION AND AUTHENTICATION CLASS: TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

FAMILY: INCIDENT RESPONSE CLASS: OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information to appropriate authorities.

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting

of security incidents. The support resource is an integral part of the organization's incident response capability.

FAMILY: MAINTENANCE CLASS: OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

MA-2 CONTROLLED MAINTENANCE

Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

MA-4 REMOTE MAINTENANCE

Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

MA-5 MAINTENANCE PERSONNEL

Control: The organization allows only authorized personnel to perform maintenance on the information system.

*MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.

FAMILY: MEDIA PROTECTION CLASS: OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

MP-2 MEDIA ACCESS

Control: The organization restricts access to information system media to authorized individuals.

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media within controlled areas.

MP-5 MEDIA TRANSPORT

Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION CLASS: OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization’s assessment of risk.

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency].

*PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

*PE-10 EMERGENCY SHUTOFF

Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

*PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

*PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

*PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

*PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

*PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.

PE-17 ALTERNATE WORK SITE

Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

FAMILY: PLANNING CLASS: MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

PL-2 SYSTEM SECURITY PLAN

Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

PL-4 RULES OF BEHAVIOR

Control: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

*PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

FAMILY: PERSONNEL SECURITY CLASS: OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

FAMILY: RISK ASSESSMENT CLASS: MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

RA-3 RISK ASSESSMENT

Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

RA-5 VULNERABILITY SCANNING

Control: The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.

FAMILY: SYSTEM AND SERVICES ACQUISITION CLASS: MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

SA-2 ALLOCATION OF RESOURCES

Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the installation of software by users.

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization designs and implements the information system using security engineering principles.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION CLASS: TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

SC-4 INFORMATION REMNANCE

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

SC-13 USE OF CRYPTOGRAPHY

Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

*SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

SC-18 MOBILE CODE

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.

*SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

*SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Control Enhancements: None.

FAMILY: SYSTEM AND INFORMATION INTEGRITY CLASS: OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection.

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

*SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

*SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

*SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**EXHIBIT 5**

**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 6

## DATA WAREHOUSE CONCEPTS & SECURITY REQUIREMENTS

### Purpose

The purpose of this document is to provide an overview of Data Warehousing and data storage concepts and to define the security requirements necessary to protect these environments. While some security controls may appear redundant to those contained in the Publication 1075, this is necessary to allow Exhibit 7 to be used as a stand-alone document. As a rule, all requirements contained within the main text of Publication 1075 will also apply to any Data Warehousing environments that are being used by Federal, state, or local agencies and these environments incorporate FTI. This will apply to authorized third parties or contractors who accept Federal Tax Information (FTI).

This document is intended to describe the controls that are specific to Data Warehousing-type environments. As the term Data Warehousing is used, the concepts will be applied to all complex data environments, including Data Warehousing, data mining, and data marts.

### Audience

This document is intended for Federal, State, and local agencies, as well as contractor personnel and third party personnel who use FTI. The document is to be used as a planning document and is intended to support the development and deployment of Data Warehousing architectures and/or architectures of a similar environment, such as Data Marts.

### Background

The IRS often uses specialized taxpayer data resources for the purpose of research, trend analysis, and specialized studies which enhance the agency's ability to recommend changes and improvements to the tax code, and for other purposes. These resources may take the form of Data Warehouses (DW) and Data Marts (DM) solutions. Similarly, Federal, State, and local agencies may use the data warehousing opportunities to improve tax code compliance or to conduct similar research, trend analysis, and specialized studies.

A Data Warehouse is a structure that is designed to distribute data from multiple arenas to the primary enterprise system. A DW collects, extracts, transforms, transports, and loads data for a distribution to various DM. A Data Mart is a structure designed for access, which is used to facilitate client user support.

In the context of FTI within agencies, the DW stores sets of historical data, which contains specific taxpayer information, as well as summary information and historical data.

A DW concept is different from a traditional networked enterprise in four ways: 1) a DW is subject oriented instead of application oriented; 2) has its data summarized instead of detailed, 3) is analysis driven instead of transaction driven, and 4) has general all-inclusive data structures rather than narrow, restricted data structures.

A DW is structured to separate analysis work from transaction work and allows large amount of data to be consolidated from several sources. The security controls remain constant with operational enterprises and will be applicable to a DW.

In a DW the scope of security changes for the different dimensions of data management. Information enters a DW through a staging area where it goes through a process of extraction, transformation, and loading. This is referred to as Extract/Transform/Load (ETL). Additionally, a DW is operated by query or search engine tool. The use of end-to-end security, the Data Warehouse ensures the confidentiality, privacy and integrity of FTI. The security of the Data Warehouse should include all aspects of the warehouse, including hardware, software, data transport, and data storage.

**Data Warehousing Implications**

FTI placed in a Data Warehouse environment may only be used for "tax administration" purpose or for other authorized purposed defined within Publication 1075. As part of the Data Warehouse, FTI data must retain its identity as FTI (i.e., it must be obvious that the IRS is the source of the data). Whenever calculations or data manipulations are being performed that could commingle FTI with any other data, the access to the FTI must be restricted to agency staff with a need-to-know and their contractors/agents as authorized by law. This is defined in the primary publication but is being reinforced for clarification.

**Security**

Security controls for Data Warehousing concepts are derived from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. These controls address the areas of management, operational, and technical controls.

When all controls are implemented and managed, these controls provide effective safeguards for the confidentiality, integrity reliability, and availability of the data. For this document, the defined controls have been mapped to the classes and families of the NIST SP 800-53 to allow technical personnel to easily review NIST controls and understand how these apply to security environments.

The next sections will define specific controls related to Data Warehousing environments. If no additional controls are required, the section will identify this fact. These controls provide unique controls for Data Warehousing environments. Otherwise, the requirements in Publication 1075 will apply.

**Management Controls**

The following section identifies high-level management controls that shall be used within a data warehousing environment.

**Risk Assessment:**

The agency shall have a Risk Management Program in place to ensure each program is assessed for risk. Risks of the data warehousing environments shall be assessed. Any risk documents shall identify and document all vulnerabilities, associated with the Data Warehousing environment.

**Planning:**

Planning is crucial to the development of a new environment. A Security Plan shall be in place to address organizational policies, security testing, rules of behavior, contingency plans, architecture/network diagrams, and requirements for security reviews. While the plan will provide planning guidelines, this will not replace requirements documents, which contain specific details and procedures for security operations.

Policies and procedures are required to define how activities and day-to-day procedures will occur. This will contain the specific policies, relevant for all of the security disciplines covered in this document. As this relates to data warehousing, any Data Warehousing

documents can be integrated into overall security procedures. A section shall be dedicated to data warehouses to define the controls specific to that environment.

Develop policies and procedures to document all existing business processes. Ensure that roles are identified for the organization, regarding the specific roles being created and the responsibilities for these roles.

Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing.

Define how “legacy system data” will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the ETL transformation process.

The policy shall ensure that FTI will not be subject to Public Disclosure. Only clients or end users can query FTI data with a concrete “need to know”.

**System and Services Acquisition:**

Acquisition security needs to be explored. As FTI is used within data warehousing environments, it will be important that the services and acquisitions have adequate security in place, including blocking information to contractors, where these contractors are not authorized to access FTI.

**Certification, Accreditation, and Security Assessments:**

Certification, accreditation, and security and risk assessments are accepted best practices used to ensure that appropriate levels of control exist, are being managed and are compliant with all Federal and State laws or statutes.

State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in NIST SP 800-53, February 2005. The process or policy must contain the methodology being used by the State or local agency to inform management, define accountability and address known security vulnerabilities.

Risk assessments should follow the guidelines provided in NIST Publication 800-30 Risk Management Guide for Information Technology Systems, July 2002.

**Operational Controls**

The following section identifies high-level operational controls that shall be used within a Data Warehousing environment:

**Personnel Security**

Personnel clearances may vary from agency to agency. As a rule, personnel with access to FTI shall have a completed background investigation. In addition, when a staff member has administrator access to access the entire set of FTI records, additional background checks may be determined necessary. All staff interacting with DW and DM resources are subject to background investigations in order to ensure their trustworthiness, suitability, and work role need-to-know. Access to these resources must be authorized by operational supervisors, granted by the resource owners, and audited by internal security auditors.

**Physical Security and Environmental Protection**

There are no special physical security controls for a Data Warehousing environment.

**Contingency Planning**

On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. By using new technologies, agencies will ensure the data being provided is reliable. As necessary, based upon risk and cost, these tools shall be implemented.

Both incremental and special purpose data back-up procedures are affected, accompanied by off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy, and are tested and verified. Though already addressed in the Publication 1075, this needs to be evaluated to ensure that all data resources are synchronized and restored to allow recreation of the data to take place.

**Configuration Management**

The agency shall have a process and documentation to identify and analyze how existing FTI is used and how FTI is queried or targeted by end users. FTI parts of the system shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. During the life cycle of the DW, on-line and architectural adjustments and changes will occur. The agency shall document these changes and assure that FTI is always secured from unauthorized access or disclosure.

**Maintenance**

There are no unique maintenance requirements for Data Warehousing environments.

**System and Information Integrity**

There are no unique system and information integrity requirements for Data Warehousing environments.

**Media Protection**

The agency shall have policy and procedures in place describing the Cleansing Process at the staging area and how the ETL process cleanses the FTI when it is extracted, transformed and loaded. Additionally, describe the process of object re-use once FTI is replaced from data sets. IRS requires all FTI is removed by a random overwrite software program.

**Incident Response**

Intrusion detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data.

**Awareness & Training**

The agency shall have a “training program” in place that will include how FTI security requirements will be communicated for end users. Training shall be user specific to ensure all personnel receive appropriate training for a particular job, such as training required for administrators or auditors.

**Technical Controls**

The following section identifies high-level technical controls that shall be used within a data warehousing environment.

**Identification & Authentication**

The agency shall configure the web services to be authenticated before access is granted to users via an authentication server.

Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure only authorized personnel have access to FTI information.

Authentication shall be required both at the operating system level and at the application level, when accessing the data warehousing environment.

**Access Control**

Access to systems shall be granted based upon the need to perform job functions.

Agencies shall identify which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure only authorized personnel have access to the areas containing FTI.

The agency shall have security controls in place that include preventative measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know there is an attack occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations.

Within the DW, the agency shall protect FTI as sensitive data and be granted access to FTI for the aspects of their job responsibility. The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job. The agency shall set up access controls in their DW based on personnel clearances. Access controls in a data warehouse are generally classified as 1) General Users; 2) Limited Access Users; and 3) Unlimited Access Users. FTI shall always fall into the Limited Access Users category.

All FTI shall have an owner assigned so that there is responsibility and accountability in protecting FTI. Typically, this role will be assigned to a management official such as an accrediting authority.

The agency shall configure control files and datasets to enable the data owner to analyze and review both authorized and unauthorized accesses.

The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be done at the authentication server.

Web-enabled application software shall:

1. Prohibit generic meta-characters from being present in input data
2. Have all database queries constructed with parameterized stored procedures to prevent SQL injection
3. Protect any variable used in scripts to prevent direct OS commands attacks
4. Have all comments removed for any code passed to the browser
5. Not allow users to see any debugging information on the client, and

6. Be checked before production deployment to ensure all sample, test and unused files have been removed from the production system.

**Audit & Accountability**

The agency shall ensure that audit reports are created and reviewed for data-warehousing-related access attempts.

A data warehouse must capture all changes made to data, including: additions, modifications, or deletions. If a query is submitted, the audit log must identify the actual query being performed, the originator of the query, and relevant time/stamp information. For example, if a query is made to determine the number of people making over $50,000, by John Doe, the audit log would store the fact that John Doe made a query to determine the people who made over $50,000. The results of the query are not as significant as the types of query being performed.

**System & Communication Protection**

Whenever FTI is located on both production and test environments, these environments will be segregated. This is especially important in the development stages of the data warehouse.

All Internet transmissions will be encrypted using HTTPS protocol utilizing Secure Sockets Layer (SSL) encryption based on a certificate containing a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This will allow information to be protected between the server and the workstation. During the Extract, Transform and Load stages of data entering a warehouse, data is at its highest risk. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption, i.e., from workstation to point of data.

Web server(s) that receive online transactions shall be configured in a “Demilitarized Zone” (DMZ) in order to receive external transmissions but still have some measure of protection against unauthorized intrusion.

Application server(s) and database server(s) shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers.

Transaction data shall be “swept” from the web server(s) at frequent intervals consistent with good system performance, and removed to a secured server behind the firewalls, to minimize the risk that these transactions could be destroyed or altered by intrusion.

Anti-virus software shall be installed and maintained with current updates on all servers and clients that contain tax data.

For critical online resources, redundant systems shall be employed with automatic failover capability.

**EXHIBIT 7**

**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 the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. 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.

**Exhibit 8**

**PASSWORD MANAGEMENT GUIDELINES**

| Control No. | Password Management Guidance |
|---|---|
| 01 | Passwords shall be a minimum length of 8 characters in a combination of alpha and numeric or special characters. |
| 02 | Passwords shall be changed every 90 days, at a minimum, for standard user accounts to reduce the risk of compromise through guessing, password cracking or other attack & penetration methods. |
| 03 | Passwords shall be changed every 60 days, at a minimum, for privileged user accounts to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods. |
| 04 | Password changes for standard and privileged users shall be systematically enforced where possible. |
| 05 | Passwords shall be systematically disabled after 90 days of inactivity to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods. |
| 06 | Users shall be prohibited from using their last six passwords to deter reuse of the same password. |
| 07 | Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change. |
| 08 | Privileged users shall be able to override the minimum password age limit for users when necessary to perform required job functions. |
| 09 | The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires. |
| 10 | User account lockout feature shall disable the user account after 3 unsuccessful login attempts. |
| 11 | Account lockout duration shall be permanent until an authorized system administrator reinstates the user account. |
| 12 | Default vendor passwords shall be changed upon successful installation of the information system product. |
| 13 | System initialization (boot) settings shall be password-protected. |
| 14 | Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen. |
| 15 | Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system. |
| 16 | Null passwords shall be prohibited to reduce the risk of compromise through rogue enticement techniques or other attack and penetration methods. |

| Control No. | Password Management Guidance |
|---|---|
| 17 | Use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords shall be prohibited when possible. Obvious combinations of letters and numbers include first names, last names, initials, pet names, user accounts spelled backwards, repeating characters, consecutive numbers, consecutive letters, and other predictable combinations and permutations. |
| 18 | Users shall commit passwords to memory, avoid writing passwords down and never disclose passwords to others (e.g., with a co-worker in order to share files). |

**Exhibit 9**

**SYSTEM AUDIT MANAGEMENT GUIDELINES**

| *Event No.* | *System Auditing Guidance* |
|---|---|
| 01 | The audit trail shall capture all successful login and logoff attempts. |
| 02 | The audit trail shall capture all unsuccessful login and authorization attempts. |
| 03 | The audit trail shall capture all identification and authentication attempts. |
| 04 | The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users). |
| 05 | The audit trail shall capture all actions, connections and requests performed by privileged functions. |
| 06 | The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions). |
| 07 | The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. |
| 08 | The audit trail shall capture the creation, modification and deletion of objects including files, directories and user accounts. |
| 09 | The audit trail shall capture the creation, modification and deletion of user accounts and group accounts. |
| 10 | The audit trail shall capture the creation, modification and deletion of user account and group account privileges. |
| 11 | The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event. |
| 12 | The audit trail shall capture system startup and shutdown functions. |
| 13 | The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s). |
| 14 | The audit trail shall capture the enabling or disabling of audit report generation services. |
| 15 | The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, database). |
| 16 | The audit trail shall be protected from unauthorized access, use, deletion or |

| *Event No.* | *System Auditing Guidance* |
|---|---|
| | modification. |
| 17 | The audit trail shall be restricted to personnel routinely responsible for performing security audit functions. |

**EXHIBIT 10**

**IRC SEC. 7213 and 7213A 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 11**

***ENCRYPTION STANDARDS***

**Federal Security Standards**

- The Digital Encryption Standard (FIPS 46-3)
- Computer Data Authentication (FIPS 113)
- Security Requirements for Cryptographic Modules (FIPS 140-2)
- Key Management Using ANSI X9.17 (FIPS 171)
- The Digital Hash Standard (FIPS 180-1)
- Secure Hash Standard (FIPS 180-2)
- Escrowed Encryption Standard (FIPS 185)
- The Digital Signature Standard (FIPS 186-2)
- Public Key Cryptographic Entity Authentication Mechanism (FIPS 196)
- Advanced Encryption Standard (FIPS 197)

**Industry Security Standards**

- Digital Certificate (ANSI X5.09)
- Public Key Cryptography 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**

- Key Management Using ANSI X9.17 (FIPS 171)
- Financial Institution Key Management (ANSI X9.17)

Note: The Federal Security Standards above are based on the Federal Information Security Management Act of 2002 (FISMA) P.L. 107-347 Title III, OMB A-130.

FIPS publications are sold by the National Technical Information Services, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161 and are available on-line at http://csrc.nist.gov.

**Exhibit 12**

**GLOSSARY - KEY TERMS AND DEFINITIONS**

A

ACCOUNTABILITY: A process of holding users responsible for actions performed on an information system.

ADEQUATE SECURITY: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

ALTERNATE WORK SITE: Any working area that is attached to the Wide Area Network (WAN) either through a Public Switched Data Network (PSDN) or through the Internet.

ASSURANCE: A measure of confidence that management, operational and technical controls are operating as intended and achieving the security requirements for the system.

ASSURANCE TESTING: A process used to determine if security features of a system are implemented as designed, and are adequate for the proposed operating environment. This process may include hands-on functional testing, penetration testing, and/or verification.

AUDIT: An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; ensure compliance with established policy and operational procedures; and recommend changes in controls, policy, or procedures where needed.

AUDIT TRAIL: A chronological record of system activities sufficient to enable the reconstruction, reviewing and examination of security events related to an operation, procedure or event in a transaction, from its inception to final results.

AUTHENTICATION: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. See IDENTIFICATION.

AUTHORIZATION: Access privileges granted to a user, program or process.

AVAILABILITY: Timely, reliable access to information and information services for authorized users.

B

BANNER: Display of an information system outlining the parameters for system or information use.

BASELINE SECURITY REQUIREMENTS: A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

C

CLASSIFIED INFORMATION: National security information classified pursuant to Executive Order 12958.

COMPROMISE: The disclosure of sensitive information to persons not authorized to receive such information.

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure.

CONFIGURATION MANAGEMENT: A structured process of managing and controlling changes to hardware, software, firmware, communications and documentation throughout the system development life cycle.

COUNTERMEASURES: Actions, devices, procedures, mechanisms, techniques, or other measures that reduce the vulnerability of an information system.

CRYPTOGRAPHY: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

D

DATA: A representation of facts, concepts, information or instruction suitable for communication, processing or interpretation by people or information systems.

DECRYPTION: The process of converting encrypted information into a readable form. Also called deciphering.

DIGITAL SUBSCRIBER LINE: A public telecommunications technology delivering high bandwidth over conventional copper wire covering limited distances.

DISCRETIONARY ACCESS CONTROL: A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups or processes.

E

ENCRYPTION: See CRYPTOGRAPHY.

ENCRYPTION ALGORITHM: A formula used to convert information into an unreadable format.

ENTERPRISE LIFE CYCLE: A robust methodology used to implement business change and information technology modernization.

EXTERNAL NETWORK: Any network residing outside the security perimeter established by the telecommunications system.

EXTRANET: A private data network using the public telephone network to establish a secure communications medium among authorized users (e.g., organization, vendors, business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases where both parties may be benefit from exchanging information quickly and privately.

F

FILE PERMISSIONS: A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

FILE SERVER: A local area network computer dedicated to providing files and data storage to other network stations.

FIREWALL: Telecommunication device used to regulate logical access authorities between network systems.

FIRMWARE: Microcode programming instructions permanently embedded into the Read Only Memory (ROM) control block of a computer system. Firmware is a machine component of computer system, similar to a computer circuit component.

G

GATEWAY: Interface providing compatibility between heterogeneous networks by converting transmission speeds, protocols, codes or security rules. This is sometimes referred to as a protocol converter.

H

HOST: A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers or servers providing Dynamic Host Configuration Protocol (DHCP) services.

I

IDENTIFICATION: A mechanism used to request access to system resources by providing a recognizable unique form of identification such as a loginid, userid or token. See AUTHENTICATION.

INFORMATION: See DATA.

INFORMATION SYSTEM: A collection of computer hardware, software, firmware, applications, information, communications and personnel organized to accomplish a specific function or set of functions under direct management control.

INFORMATION SYSTEM SECURITY: The protection of information systems and information against unauthorized access, use modification or disclosure -- ensuring confidentiality, integrity and availability of information systems and information.

INTEGRITY: Protection of information systems and information from unauthorized modification; ensuring quality, accuracy, completeness, non-repudiation and authenticity of information.

INTERNET: Two or more networks connected by a router; the world's largest network using TCP/IP to connect government, university and commercial institutions.

INTRANET: A private network using TCP/IP, the Internet and world-wide-web technologies to share information quickly and privately between authorized user communities, including organizations, vendors and business partners.

K

KEY: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

LEAST PRIVILEGE: A security principle stating users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

MANAGEMENT CONTROLS: Security controls focused on managing organizational risk and information system security, and devising sufficient countermeasures or safeguards for mitigating risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.

MALICIOUS CODE: Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity and availability of information systems and information.

N

NETWORK: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected systems. Examples of networks include local area networks, wide area networks, metropolitan area networks and wireless area networks.

NODE: A device or object connected to a network.

NON-REPUDIATION: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets. That is, senders and recipients of information can not deny their actions.

O

OBJECT REUSE: The reassignment of storage medium, containing residual information, to potentially unauthorized users or processes.

OPERATIONAL CONTROLS: Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.

ORGANIZATION: An agency or, as appropriate, any of its operational elements.

P

PACKET: A unit of information traversing a network.

PASSWORD: A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

PENETRATION TESTING: A testing method where security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

PERSONALLY IDENTIFIABLE INFORMATION: Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

PLAN OF ACTION AND MILESTONES (POA&M): A management tool used to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems. (Defined in OMB Memorandum 02-01)

POTENTIAL IMPACT: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

PROTOCOL: A set of rules and standards governing the communication process between two or more network entities.

R

REMNANTS: Residual information remaining on storage media after reallocation or reassignment of such storage media to different organizations, organizational elements, users or processes. See OBJECT REUSE.

RESIDUAL RISK: Portions of risk remaining after security controls or countermeasures are applied.

RISK: The potential adverse impact to the operation of information systems affected by threat occurrences on organizational operations, assets and people.

RISK ASSESSMENT: The process of analyzing threats to and vulnerabilities of an information system to determining the potential magnitude of harm, and identify cost-effective countermeasures to mitigate the impact of such threats and vulnerabilities.

RISK MANAGEMENT: The routine process of identifying, analyzing, isolating, controlling, and minimizing security risk to achieve and maintain an acceptable risk level. A risk assessment is an instrumental component of the risk management life cycle.

S

SAFEGUARDS: Protective measures prescribed to enforce the security requirements specified for an information system. This is synonymous with security controls and countermeasures.

SECURITY POLICY: The set of laws, rules, directives and practices governing how organizations protect information systems and information.

SECURITY REQUIREMENT: The description of a specification necessary to enforce the security policy. See BASELINE SECURITY REQUIREMENTS.

SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (USC) (the Privacy Act of 1974), but which has not been specifically authorized under criteria established by an Executive Order (E.O.) or Congress to be kept secret in the interest or national defense for foreign policy.

SYSTEM: See INFORMATION SYSTEM.

SYSTEM SECURITY PLAN: An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-18)

T

TECHNICAL CONTROLS: Security controls executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

THREAT: An activity, event or circumstance with the potential for causing harm to information system resources.

U

USER:  A person or process authorized to access an information system.

USER IDENTIFIER: A unique string of characters used by an information system to identify a user or process for authentication.

V

VIRUS:  A self-replicating, malicious program that attaches itself to executable programs.

VULNERABILITY:  A known deficiency in an information system that threat agents can exploit to gain unauthorized access to sensitive or classified information.

VULNERABILITY ASSESSMENT:  Systematic examination of an information system to determine its' security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

This page intentionally blank.

This page intentionally blank.

This page intentionally blank.

Department of the Treasury
**Internal Revenue Service**
publish.no.irs.gov
Publication 1075 (10-2007)
Catalog Number 46937O