Publication 1075

Tax Information Security Guidelines For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns and Return Information

IRS

TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES 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 (October 2007).

This page left intentionally blank.

HIGHLIGHTS FOR 2010

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, revision 3. 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, 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 received, processed, 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

Correspondence, reports, attachments, requests for technical assistance, requests for current templates, etc., should be emailed to the Safeguard mailbox: SafeguardReports@irs.gov.

Safeguards recommends that all required reports be submitted using IRS approved encryption methods.

INTERNET ACCESS

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

The IRS.gov website contains guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements. URL: http://www.irs.gov/businesses/small/article/0,,id=177651,00.html

REPORTING UNAUTHORIZED DISCLOSURES

Unauthorized inspection or disclosure of Federal tax information, including breeches and security incidents, must be reported immediately to the appropriate Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards using the procedures outlined in section 10.0

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. The Federal tax regulation 26 CFR 301.6103(p)(7)-1 establishes a consistent appeal process for all authorized recipients of FTI. See Exhibit 3.

This page left intentionally blank.

TABLE OF CONTENTS

This page left intentionally blank.

1.1 General

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), which is a felony offense. 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 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.

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.

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 as a condition of receipt of FTI.

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.

Requirements throughout Publication 1075 apply to all organizational segments of an agency receiving FTI. It is the agency's responsibility to ensure all functions within their agency, including consolidated data centers and contractors (where allowed by federal statute), with access to FTI understand and implement the Publication 1075 requirements.

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 14 are provided for additional guidance.

The IRS Office of Safeguards is responsible for all interpretations of safeguarding requirements. Publication 1075 requirements may be supplemented or modified between editions of Publication 1075 via guidance issued by the Office of Safeguards and posted on their IRS.gov web site.

The IRS.gov website contains guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements. URL: http://www.irs.gov/businesses/small/article/0,,id=177651,00.html

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 1, *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 must be followed up by submitting an SPR. It must 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, divisions or programs within one agency using FTI may be consolidated into a single report for that agency, with permission of the Office of Safeguards. Entering into any agreement for disclosure to agents or contractors of an agency requires advance notice to the Office of Safeguards (see section 11.3)

An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Enterprise security policies 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.

The Office of Safeguards conducts “need and use” reviews as part of the safeguard review and always considers if the agency’s

use is in conformance with the governing provisions allowing the disclosure of FTI.

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 secures the data during transmission and has replaced the distribution of magnetic tape cartridges by the IRS.

2.4 State Tax Agency Limitations

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 should include some account of the result of its use of FTI (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 and discuss the need to stop disclosures so they no longer receive this FTI. In conformance with IRC 6103(d), 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 tax administration purposes.

State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must notify the IRS by submitting a signed *Need and Use Justification for Use of Federal Tax Information for Tax Modeling, Revenue Estimation or Other Statistical Purposes* and following the established guidelines.

Annually, the agency will provide updated information regarding their modeling activities which include FTI in their Safeguard Activity Report. In the annual SAR, the agency must describe:

- any use of FTI that is in addition to what was described in the original Need and Use Justification
- any new, previously unreported internal tax administration compilations that include FTI
- Changes to the listing of authorized employees (Attachment B to the Need and Use Justification)

If the agency intends to use a contractor for conducting statistical analysis, tax modeling or revenue projections, they must submit a 45-day notification (see section 11.3) prior to contractor access to the FTI. The agency's Safeguard Procedures Report should detail the use of FTI for this purpose. In addition, the agency must submit a separate statement detailing the methodology used and data to be used by the contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that appropriate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information, is appropriate.

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 safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official(s) 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(s) should also be responsible for ensuring that internal inspections are

conducted, for submitting required safeguard reports to the IRS, for properly reporting any data breach incidents, 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 Office of Communication, Liaison, and Disclosure Office (CLD:S).

2.7 Conducting the Review

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

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.

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 (covering employee awareness and internal inspections), Reporting Requirements, and Disposal. Computer Security and Need and Use are a part of Restricting Access but 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 conference 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 closing conference when the agency is informed of preliminary findings identified during the evaluation. An interim Safeguard Review Report (SRR) will be issued to document the on-site review findings.

The agency must respond to the interim SRR by submitting a Corrective Action Plan (CAP), detailing their planned actions to resolve the identified findings. Once the agency's response to the interim SRR is received, a final SRR will be issued.

The agency's response to the interim SRR includes the submission of the initial Corrective Action Plan (CAP). The CAP must be updated and submitted to the Office of Safeguards twice a year until all review findings are accepted and closed by the Office of Safeguards.

The CAP must include a brief explanation of actions already taken or planned to resolve the finding. For all outstanding findings, the agency must detail planned actions and associated milestones for resolution.

All findings should be addressed in a timely fashion. The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues should be resolved and addressed in the next reporting cycle of the Corrective Action Plan (CAP), Safeguard

Activity Report (SAR), or, if necessary, the Safeguard Procedures Report (SPR) (see section 7.0).

Guide 1 – Safeguard Review Cycle

Preliminary Discussions
Engagement Letter
Opening Conference
On-site Evaluation
Closing Conference (with Preliminary Findings)
Interim Report
Agency Response (Initial Corrective Action Plan (CAP))
Final Report
CAP Submissions Until All Findings Resolved

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 from receipt through destruction. 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
- 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.

Responsible officials must ensure that electronic media containing FTI removed from the storage area is properly recorded on charge-out records. Semi-annual inventories of removable media must be conducted. The agency must account for any missing electronic media, document search efforts taken and notify the appropriate authorities as directed in section 10.0 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 electronic media, document search efforts taken and notify the appropriate authorities as directed in section 10.0 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 human services agencies 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 Converted Media

Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) also requires tracking from creation to destruction of the converted FTI. All converted FTI should be tracked on logs containing the data elements detailed in sections 3.2 and 3.3 above, depending upon the current form of the FTI. Paper to electronic FTI logs shall reflect the data elements in section 3.2 and electronic media to paper FTI logs shall reflect the data elements in section 3.3.

3.5 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 electronic 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.

Disclosure of FTI to state auditors by child support enforcement and human services agencies is statutorily prohibited if the state auditors are not employed by the state. If the state auditors are contractors instead of state employees, the disclosure restrictions pertaining to contractors or agents apply. Whenever possible, FTI in case files should be removed prior to access by the auditors.

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 – Secure Storage, Physical Security – Minimum Protection Standards, within this document, should be used as an aid in determining the method of safeguarding federal tax information. 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 physically protecting data and systems that require safeguarding. This method 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 physical security needs at individual facilities. The MPS have 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 with controlled access to the keys or combinations. A security container is a lockable metal container with a resistance to forced penetration, with a security lock with controlled access to keys or combinations. (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 or landlords for non-government owned facilities 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, custodial services worker or landlord 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, janitor or landlord may have a key to the building but not the room.

During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed, preferably worn above the waist.

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 federal tax information 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.

A restricted area visitor log 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. The entry control monitor or escort must identify the type of identification used to verify the identity of the visitor on the visitor log. 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 visitor log. 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 contain FTI. This shall not apply to those areas within the facility officially designated as publicly accessible.

The site shall issue appropriate authorization credentials. The agency shall

issue authorization credentials to include badges, identification cards and/or smart cards. 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)

The agency shall control physical access to information system distribution and transmission lines within the organizational facilities. (Exhibit 4, PE-4)

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 must contain the following information:

- name and organization of the visitor
- signature of the visitor
- form of identification
- date of access
- time of entry and departure
- purpose of visit
- 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 authorize and control information system-related items entering and exiting the facility and maintain 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 locked 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 federal tax information 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. 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 receive, store, process and transmit, 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 3.0, *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 receive, process, access, and store FTI. The agency must retain ownership and control, for all hardware, software, and end-point 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-06-16).

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 9.17.3, 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*).

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 2, *Sec. 6103(p)(4) Safeguards* and Exhibit 6*, 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 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 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 electronic 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 9.0, *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 the 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 application, databases, data profiles, data tables, or data columns and rows, and data elements. The FTI within any of the above must 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.

When an agency implements a data warehouse containing FTI, the agency must provide written notification to the IRS Office of Safeguards, identifying the security controls, including FTI identification and auditing within the data warehouse. The written notification shall be sent to the SafeguardReports@IRS.gov mailbox at least 45 days before implementation. In addition, implementation of a data warehouse constitutes a significant change under section 7.1, triggering the requirement for the submission of a new SPR. See Exhibit 11, *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 FTI. "Provided" means actually giving the information on a separate document, not just verifying and returning a document that includes FTI.
- If a new address is received from Internal Revenue Service records and entered into a computer database, the address must be identified as FTI and safeguarded. If the individual or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten by replacing the IRS source address with the newly provided information, non-IRS source address. Again, "provided" means using the individual's or third party's knowledge or records as the source of information, which does not include FTI.

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. Questions about whether particular state employees are entitled to have access FTI, should be forwarded to the Disclosure Manager at the IRS Office that serves your location. Generally, the IRC does not permit state tax agencies to furnish FTI to other state agencies or to political subdivisions, such as cities or counties. State tax agencies may not furnish FTI to any other state or local agency, even where agreements have been made, informally or formally, for the reciprocal exchange of state tax information unless formally approved by the IRS. 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, absent explicit IRS authority granted under IRC 6103(p)(2)(B).

Although state tax agencies are specifically addressed above, the restrictions on data access and/or redisclosure to another agency or third party applies to all agencies authorized to receive FTI. Generally, statutes that authorize disclosure of FTI do not authorize further disclosures by the recipient agency. Unless IRC Section 6103 provides for further disclosures by the agency, the agency cannot make such disclosures or otherwise grant access to FTI to employees of another component of the agency not involved with administering the program for which the FTI was specifically received, or to another state agency for any purpose.

Agencies and subdivisions within an agency may be authorized to obtain the same FTI for the different purposes, such as a state tax agency administering tax programs and a component human services agency administering benefit eligibility verification programs (IRC Section 6103(l)(7)) and/or child support enforcement programs (IRC Section 6103(l)(6)). However, the Internal Revenue Code disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information for another authorized purpose even within the agency.

In addition, unless specifically authorized by the IRC, agencies are not permitted to allow access to FTI to agents, representatives or contractors.

FTI may not be accessed by agency employees, agents, representatives or contractors located “offshore”, outside of the United States or its territories. Further, FTI may not be received, stored, processed or disposed via information technology systems located off-shore.

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, digital images or hard copy printout) will be performed pursuant to one of the following 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 – Consolidated Data Centers

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.

Note: For purposes of applying sections 6103(l), (m) and (n), the term "agent" includes contractors.

Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center.

The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 6103(n).

The contractor or agency-shared computer facility is also subject to IRS safeguard reviews.

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.

Agencies utilizing consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA should cover the following:

- The consolidated data center is considered to be a "contractor" of the agency receiving FTI. The agency receiving FTI – whether it is a state revenue, workforce, child support enforcement or human services agency – is responsible for ensuring the protection of all FTI received. However, as the "contractor" for the agency receiving FTI, the consolidated data center shares responsibility for safeguarding FTI as well.

- Provide written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all federal tax information within their possession or control. The SLA should also include details concerning the consolidated data center's responsibilities during a safeguard review and support required to resolve identified findings.

- The agency will conduct an internal inspection of the consolidated data center every eighteen months (see section 6.3). Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care should be taken to ensure agency representatives do not gain unauthorized access to other agency's FTI during the internal inspection.

- The employees from the consolidated data center with access to FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the consolidated data center that has access to FTI.

- The specific data breach incident reporting procedures for all consolidated data center employees and contractors. The required disclosure awareness training must include a review of these procedures.

- The Exhibit 7 language must be included in the contract between the

recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.

- Identify responsibilities for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

Note: Generally, consolidated data centers are either operated by a separate state agency (example: Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision-making or implementation planning process. The purpose of these discussions is to ensure the agency remains in compliance with safeguarding requirements during the transition to the consolidated data center.

5.6 State and Local Child Support Enforcement Agencies IRC Section 6103(l)(6), (l)(8) and (l)(10)

In general, no officer or employee of any State and local child support enforcement agency can make further disclosures of FTI.

However, limited information may be disclosed 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 for this purpose to an agent or a contractor is limited to:

- the address

- social security number 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.

Tax refund offset payment information may not be disclosed by any federal, state or local child support enforcement agency employee, representative, agent or contractor into any court proceeding. To satisfy the redisclosure prohibition, submit only payment date and payment amount for all payment sources (not just tax refund offset payments) into court proceedings.

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

5.7 Federal, State, and Local Human Services 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 for any purpose. Human Services agencies may not contract for services that involve the disclosure of FTI to contractors.

5.8 Deficit Reduction Agencies IRC Section 6103(l)(10)

Agencies receiving FTI from the Financial Management Service related to tax refund offsets are prohibited from making further disclosures of the FTI received to another agency or to contractors.

5.9 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.

5.10 Disclosures Under IRC Section 6103(l)(20)

Disclosures to officers, employees and contractors of the Social Security Administration and other specified agencies are authorized to receive specific tax information for the purpose of carrying out the Medicare Part B premium subsidy adjustment and Part D Base Beneficiary Premium Increase. These disclosures are subject to safeguards requirements. Any agency receiving FTI from SSA authorized by this provision is also subject to IRS safeguard requirements and review.

5.11 Disclosures Under IRC Section 6103(l)(21)

Disclosures to officers, employees and contractors of the Department of Health and Human Services, an Exchange or a state agency are authorized to receive specific tax information for the purposes of establishing eligibility for participation in the Exchange, verifying the appropriate amount of any credits and determining eligibility for participation in the state program. These disclosures are subject to safeguards requirements. Any agent or contractor is also subject to IRS safeguard requirements and review.

5.12 Disclosures Under IRC Section 6103(i)

Federal law enforcement agencies receiving FTI pursuant to court orders or by specific request under Section 6103(i) for purposes of investigation and prosecution of non-tax federal crimes, or to apprise of or investigate terrorist incidents, are subject to safeguard requirements and review.

The Department of Justice must report in their annual Safeguard Activity Report the number of FTI records provided and to which federal law enforcement agency the data was shared for the calendar year processing period.

5.13 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. If the FTI is shared with agents or contractors, the agency, and agent or contractor, are all subject to IRS safeguarding requirements and reviews.

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 an employee or contractor access to FTI must be preceded by certifying that each employee or contractor understands the agency's security policy and procedures for safeguarding IRS information. Employees and contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, employees and contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*).

The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See section 10.0)

For both the initial certification and the annual certification, the employee or contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

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 must 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. All contractors with access to FTI, including a consolidated data center or off-site storage facility, must also be reviewed within an 18-month cycle.

The agency should complete an internal inspection plan, detailing the timing of all internal inspections in the current year and next two years (3 year cycle). The plan must be included as part of the annual SAR (see section 7.4.2.B). 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, officers and contractors 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 9.0, *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.

6.4 Plan of Action & Milestones (POAM)

The agency must implement a process for ensuring that a Plan of Action & Milestones (POAM) is developed and monitored. The POAM will be based upon the corrective actions identified during the internal inspections and will identify the actions the agency plans to take to resolve these.

Note: The POAM pertains to findings identified by the agency during the internal inspections. The CAP covers findings identified by the Office of Safeguards during the on-site safeguard review. While these findings may be similar, their inclusion in either the POAM or CAP is dependent upon how they were identified and who (the agency or the IRS Office of Safeguards) is monitoring the finding resolution.

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 received and 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, systems or applications (hardware or software); new facilities; and organizational changes such as movement to a consolidated data center from an embedded IT operation.

Agencies entering into new data exchange agreements that authorize the receipt of new data sets containing FTI not previously received by the agency or a new use of existing FTI not already covered in the current SPR, must submit an addendum to the currently approved SPR. The addendum details the handling of the new data set within the agency. In lieu of an addendum, the agency must certify to the Office of Safeguards that the new data will be utilized and safeguarded as outlined in the existing SPR. Such certification will not extend the six year time period for submission of a new SPR.

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 obtained from IRS.GOV keyword "Safeguards" or requested by emailing 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, and dated.

Information requested on the template includes:

7.2.1 Responsible Officer(s)

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

The name, title, address, email address and telephone number of the agency official responsible for implementing the safeguard procedures, including but not limited to the agency information technology security office or equivalent and the primary IRS contact.

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 received, 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 received and 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. Indicate if FTI is commingled or where FTI may be replicated, reproduced, transcribed, duplicated, backed up, distributed or printed. Indicate all points where contactors have access to FTI.

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 Other Safeguards

A description of the process implemented to conduct all required internal inspections and address all identified findings.

7.2.8 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.

7.2.9 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 9.0). 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.

7.2.10 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

The SPR package, including the SPR template, transmittal letter and all associated attachments must be submitted electronically to: SafeguardReports@irs.gov.

Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must submit an initial SPR at least 45 days before the agency will begin receiving FTI.

Subsequent SPRs triggered by a significant change must be submitted at least 45 days before the implementation of the significant change.

Note: Paper report submissions will no longer be accepted. Reports must be submitted on the current template in Word format.

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 downloaded from IRS.GOV keyword "Safeguards" or requested by emailing 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, and dated. All sections of the template must be completed, including agency identifying information and agency code. The template includes the following sections:

7.4.1 Changes to Information or Procedures Previously Reported

A. Responsible Officers or Employees, including but not limited to agency director or commissioner; information technology security officer or equivalent; and the primary IRS contact.

B. Functional Organizations Accessing the Data, including off-site storage, consolidated data centers or disaster recovery organizations

C. Computer Facilities or Equipment and System Security – Hardware or Software Changes or Enhancements

D. Physical Security – Changes or Enhancements (space moves; new locations)

E. Retention and 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 (see section 6.4). In addition, the agency should submit the internal inspection plan required by section 6.3.

C. Disposal of FTI

Describe the amount and method of destruction for FTI (paper and/or electronic) disposed during the processing period. The description may be a summary from logs which track FTI from receipt through destruction. Copies of logs should not be submitted; a copy of the log template would suffice.

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

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

Agencies authorized to redisclose FTI to other agencies must provide the name(s) of the agency to whom they provided FTI and the number of records provided.

Note: Generally, agencies permitted to redisclose FTI will receive instructions from the Office of Safeguards on items to report.

7.4.3 Actions on Safeguard Review Recommendations

The agency should report all corrective actions taken or planned to address findings arising from the last on-site safeguard review. This will be done through submission of an updated Corrective Action Plan (CAP) as an attachment to the SAR (see section 7.5).

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 or organizational changes.

7.4.5 Agency Use of Contractors

The agency must identify all contractors with access to FTI and the purpose for which access was granted. The agency must provide the name and address of the contractor.

Note: FTI may not be accessed by contractor's employees located offshore or be included in contractor's information systems located off-shore.

7.4.6 FTI Data Received

The agency must summarize the data received, both paper and electronic, during the reporting period, including source, name of file or extract, and volume. A summary of the record keeping logs required in section 3 for electronic and paper data would meet this requirement.

7.4.7 Update of Tax Modeling Activities

State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must provide updated information regarding their modeling activities which include FTI. In the annual SAR, the agency will describe:

- The use of FTI that is in addition to what was described in the original Need and Use Justification (update of Attachment A to the Need and Use Justification)
- Any unanticipated internal tax administration compilations that include FTI
- Changes to the listing of authorized employees (Attachment B to the Need and Use Justification)

7.4.8 Submission Dates for the Safeguard Activity Report

The SAR package, including the SAR template, transmittal letter and all associated attachments must be submitted electronically using IRS approved encryption techniques. The email address used to submit all reports is: SafeguardReports@irs.gov.

Federal Agencies must submit their reports for the calendar year processing period (January 1 though December 31), by **January 31** of the following year.

State and Local Revenue Agencies (including cities, counties, local government agencies or municipalities administering income taxes), must submit their reports for the calendar year processing period (January 1 through December 31) by **January 31** of the following year.

State Child Support Enforcement Agencies must submit their reports for the annual processing period March 1 through February 28, by **March 31**.

Other State Agencies (i.e., agencies administering taxes and receiving FTI under IRC 6103(d) other than the Revenue Department), including Departments of Labor, state workforce agencies (SWA), Departments of Transportation, Motor Vehicle agencies, etc.), and Attorneys General with oversight for charitable organizations receiving FTI under IRC 6104(c), must submit their reports for the annual processing period June 1 through May 31, by **June 30**.

State Human Services Agencies administering certain public benefit eligibility programs receiving FTI under 6103(l)(7) from IRS and SSA, must submit their reports for the annual processing period September 1 through August 31, by **September 30**.

Note: Educational institutions receiving IRS addresses to locate debtors under IRC Section 6103(m)(4)(B) must send annual reports to the Department of Education as the federal oversight agency for this program.

7.5 Corrective Action Plan (CAP)

The IRS will provide each agency with a pre-populated Corrective Action Plan (CAP) along with the interim SRR. The agency must complete the CAP to specify the corrective action(s) taken, or planned, to address each finding included in the interim SRR, and the actual or planned, implementation date to resolve all identified findings from the last on-site safeguard review.

7.5.1 Submission Dates for the Corrective Action Plan

The agency must submit an initial CAP as part of the agency's response to the interim SRR. Subsequently, the agency must submit an updated CAP twice each year – biannually, as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date

Agencies must submit a CAP every six months until all corrective actions from the last review are closed by the Office of Safeguards.

Note: Depending upon the date the interim SRR was issued, the agency's first CAP update may be due before the annual due date of the next SAR.

The due date for the CAP that accompanies the annual SAR is provided in section 7.4.7. The CAP due dates are provided below. and summarized in the chart. The CAP reporting date is fixed so that the CAP is due on schedule regardless of whether the agency's SAR was timely filed:

CAP reporting dates:

Federal Agencies – July 31

State and Local Revenue Agencies including cities, counties, and local governments or municipalities – July 31

State Human Services Agencies – administering benefit eligibility programs under IRC 6103(l)(7) – March 31

State Child Support Enforcement Agencies – September 30

Other State Agencies (agencies other than the Revenue Department) – December 31

Reports must be sent encrypted via IRS approved encryption techniques. The email address for all reports is: SafeguardReports@irs.gov.

Corrective Action Plan (CAP) Due Dates

	Type	**SAR and CAP Due**	**CAP Due Date**
Federal Agencies	FED	January 31	July 31
State and Local Revenue Agencies	DOR	January 31	July 31
State IV-D Child Support Enforcement Agencies	CS	March 31	September 30
Other State Agencies	SWA, DOT, AG	June 30	December 31
State Human Services Agencies	HS	September 30	March 31

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 2, 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 from which 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 paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating.

The following precautions must 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 must be separated to ensure that all pages are consumed.

- Shredding precautions: To make reconstruction more difficult, the paper must be inserted so that lines of print are perpendicular to the cutting line and not maintain small amounts of shredded paper. The paper must be shredded to effect 5/16 inch wide or smaller strips; microfilm and microfiche must 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's 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.

Electronic media 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 physical 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

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.

When using either method for destruction, every third piece of physical electronic media should be checked to ensure appropriate destruction of FTI.

Note: Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

9.1 General

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

The 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, revision 3, *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 receiving, processing, storing and transmitting Federal tax information must be hardened in accordance with the requirements of Publication 1075. 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.

Safeguard Computer Security Evaluation Matrices (SCSEMs) provide hardening guidance for specific technologies and are available on Safeguards' IRS.gov website.

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.

9.2. 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. The agency must ensure that only authorized employees or contractors (if allowed by statute) of the agency receiving the information have access to FTI. For example, human services agencies may not have access to FTI provided to child support enforcement agencies or state revenue agencies. Management must supervise and review the activities of the users as this relates to information system access.

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 or warning banner before granting system access informing potential users that (i) the system contains U.S. Government information; (ii) users actions are monitored and audited; (iii) unauthorized use of the system is prohibited; and (iv) unauthorized use of the system is subject to criminal and civil sanctions. The warning banner must be applied at the application, database, operating system and network device level for all system types that receive, store, process and transmit FTI. (See Exhibit 13 for example warning banners)

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. Remote access is defined as any access to an agency information system by a user communicating through an external network, for example: the Internet.

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 contain FTI. Agencies must develop policies for any allowed wireless access, where these systems contain FTI. (Exhibit 4, AC-17).

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 accessing FTI.

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 receive, 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)

Note: For specific guidance on the use of web portals and IVR systems, see sections 9.18.9 and 9.18.10.

9.3 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 review, 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 requirements for creating audit-related processes at both the application and system levels. Within the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also

applies to data tables or databases embedded in or residing outside of the application.

The information system shall alert appropriate organizational officials in the event of an audit processing failure and take 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 must protect audit information and audit tools from unauthorized access, modification, and deletion. (Exhibit 4, AU-9)

9.4 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)

9.5 Security Assessment and Authorization

Note: For federal agencies that receive FTI, a NIST compliant C&A is required in accordance with FISMA. For state or local agencies that receive FTI, a third-party accreditation is not required. Instead these agencies may internally attest.

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 certification & accreditation (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. (Exhibit 4, CA-1)

The agency shall conduct, periodically but at least annually, an assessment of the security controls in the information system 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. The assessment should be documented in writing. (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. 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-3)

As recipients of FTI, the agency is responsible to develop and update a Plan of Action & Milestones (POAM) that shall identify any deficiencies related to FTI processing. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during internal inspections. The CAP will identify activities planned or completed to correct deficiencies identified during the on-site safeguard review. Both the POAM and the CAP 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 authorization 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 authorization. All information regarding the authorization 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)

9.6 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:

- 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)
- Analyze changes to the information system to determine potential security impacts prior to change implementation (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 receiving, 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)

9.7 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.

9.8 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)

9.9 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. These policies and procedures should cover both physical and information system security relative to the protection of federal tax information. Such incident response security controls include incident response training and incident reporting and monitoring.

Agencies must train personnel with access to federal tax information, including contractors and consolidated data center employees if applicable, 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 all physical and 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 document the results. (Exhibit 4, IR-3)

Any time there is a compromise to FTI, the agency must immediately report incident information to the appropriate Agent-in-Charge, TIGTA and the IRS following the requirements of section 10. (Exhibit 4, IR-6)

The agency shall also provide an incident response support resource that offers advice and assistance to users of the federal tax information and any information system containing federal tax information 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)

9.10 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)

9.11 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 must label removable media (CDs, magnetic tapes, external hard drives, flash/thumb drives, DVDs) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B can be used for this purpose. (Exhibit 4, MP-3)

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.

The agency must use transmittals or an equivalent tracking method to ensure FTI reaches its intended destination. (Exhibit 4, MP-5)

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

9.12 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.

9.13 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)

9.14 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. 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-3).

At a minimum, systems containing FTI shall be scanned quarterly to identify any vulnerabilities in the information system. The vulnerability scanning tool must be updated with the most current definitions prior to conducting a vulnerability scan. (Exhibit 4, RA-5)

9.15 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. The contract for the acquisition must contain Exhibit 7 language as appropriate. (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 agency shall perform configuration management during information system design, development, implementation, and operation; and manage and control changes to the information system. The agency shall implement only organization-approved changes, document approved changes to the information system and track security flaws and flaw resolution. (Exhibit 4, SA-10)

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

9.16 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 agency must encrypt all media containing FTI during transmission.

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 without 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)

9.17 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, information system monitoring, 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 receiving, 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, issue alerts/advisories to appropriate personnel, and take appropriate actions in response. (Exhibit 4, SI-5)

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

9.18 Additional Computer Security Controls

9.18.1 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.

section 5.3 and Exhibit 11, *Data Warehouse Concepts & Security Requirements*, provide unique requirements for this environment.

9.18.2 Transmitting FTI

All FTI data in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN).

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.

9.18.3 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 required whenever FTI is being accessed from an alternate work location or if accessing FTI via the agency's web portal.

9.18.4 Internet

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.

9.18.5 Electronic Mail

Generally, FTI should not be transmitted or used on the agency's internal e-mail systems. FTI must not be transmitted outside of the agency, either in the body of an email or as an attachment.

If transmittal of FTI within the agency's internal e-mail system is necessary, the following precautions must be taken to protect FTI sent via E-mail:

- Do not send FTI unencrypted in any email messages
- The file containing FTI must be attached and encrypted
- Ensure that all messages sent are to the proper address
- Employees should log off the computer when away from the area

9.18.6 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
  - A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.

9.18.7 Multi-Functional Printer-Copier Devices

If the agency uses a multi-functional printer-copier device, specific requirements regarding FTI must be followed.

- FTI must be encrypted in transit either to or from the device
- FTI must not be emailed or faxed from the device
- If FTI is scanned into the device, the user must authenticate on the device with a unique username and password
- FTI may not be stored locally on the device

9.18.8 Live Data Testing

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. The agency must also submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing.

9.18.9 Web Portal

To utilize a web portal that provides FTI over the Internet to a customer, the agency must meet the following requirements:

- The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI and access to the database through the application is limited.

- Each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the web portal is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.

Access to FTI via the web portal requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

9*.18.10 Integrated Voice Response (IVR) Systems*

- To utilize an IVR system that provides FTI over the telephone to a customer, the agency must meet the following requirements:

- The LAN segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system.

- The operating system and associated software for each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.

- Independent security testing must be conducted on the IVR system prior to implementation.

- Access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication

elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

9.*18.11 Emerging Technologies*

Requirements for safeguarding FTI when using emerging technologies to receive, process, store and transmit FTI will be developed by the Office of Safeguards in conformation with the applicable NIST standards. Requirements for these emerging technologies may be issued via a directive issued by the Office of Safeguards and posted to the IRS.gov web site as an addendum to the Publication 1075 (see section 1.2). Agencies planning to or in the process of implementing an emerging technology, such as cloud computing, virtualization and Voice over IP (VoIP), to receive, process, store or transmit FTI should contact the Office of Safeguards via their mailbox, SafeguardReports@IRS.gov, to request technical assistance.

REPORTING IMPROPER INSPECTIONS OR DISCLOSURES SECTION 10.0

10.1 General

Upon discovering a possible improper inspection or disclosure of FTI, including breaches 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) and the IRS (section 10.2).

TIGTA Field Division	States Served by Field Division	Telephone Number
Atlanta	Commonwealth of Puerto Rico, Virgin Islands, 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 X 104
Dallas	Kansas, Louisiana, Missouri, Nebraska, Oklahoma, Texas	(972) 308-1400
Denver	Alaska, Arizona, Colorado, Idaho, Montana, New Mexico, Nevada, Oregon, Utah, Washington, Wyoming	(303) 291-6102
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
Internal Affairs Division	Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	(202) 927-7197

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

Hotline Number: **1-800-589-3718**

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

10.2 Office of Safeguards Notification Process

Simultaneously to notifying TIGTA, the agency must notify the IRS Office of Safeguards. The TIGTA contact information is shown in section 10.1.

To notify the IRS Office of Safeguards, the agency should document the specifics of the incident known at that time into a Data Incident Report, including but not limited to:

- Name of agency and agency point of contact for resolving data incident with their contact information
- Date and time of the incident
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved. Include specific data elements if known.
- Potential number of FTI records involved. If unknown, provide a range if possible.
- Address where the incident occurred
- Information technology involved (example: laptop, server, mainframe)
- Do not include any FTI in the Data Incident report.
- Email the Data Incident Report to the SafeguardReports@IRS.gov mailbox. Reports should be sent electronically and encrypted via IRS approved encryption techniques. Use the term "Data Incident Report" in the subject line of the email.

Note: Timely notification is the most important factor, not the completeness of the Data Incident Report. Additional information will be secured via conversations with the Office of Safeguards.

The focus of the Office of Safeguards' investigation of the unauthorized access or data breach incident will be to identify processes, procedures, or systems within the agency with inadequate security controls.

10.3 Incident Response Procedures

Incident response policies and procedures required in section 9.9 should be used when responding to an identified unauthorized disclosure or data breach incident. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provided adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.

10.4 Incident Response Timeframes

The agency will contact TIGTA and the IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. The agency should not wait to conduct an internal investigation to determine if FTI was involved. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.

10.5 Incident Response Cooperation

The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident. Based upon the analysis of the incident, the agency may be required by the Office of Safeguards to modify security policy, procedure, or controls to more appropriately protect FTI in the possession of the agency. The Office of Safeguards will coordinate with the agency to ensure appropriate follow-up actions taken by the agency have been completed to ensure continued protection of FTI in the possession of the agency.

10.6 Incident Response Notification to Impacted Individuals

Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the agency's internal policy since the FTI is within the agency's possession or control. However, the agency must inform the IRS Office of Safeguards of notification activities undertaken, preferably before released to the impacted individuals. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

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.

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 45-Day Notification for Disclosing FTI to Contractors

All agencies intending to disclose federal tax information to contractors (including consolidated data centers, off-site storage facilities, shred companies, information technology support, and for tax modeling or revenue forecasting purposes) must 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. In addition, if an existing contractor employs the services of a sub-contractor, a notification is required 45-days prior to the disclosure of FTI. (See Exhibit 12 for specific data required in the 45-day notification)

The state tax agency 45-day notification regarding disclosure of FTI to a contractor for tax modeling or revenue forecasting purposes must also include a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data information to the IRS Statistics of Income for approval of the modeling methodology. (see section 2.4)

State tax authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, administering state tax laws, pursuant to Treasury Regulation 301.6103(n)-1.

Agencies receiving FTI under authority of IRC 6103(l)(7) may not disclose FTI to contractors for any purpose.

11.4 Redisclosure Agreements

In rare circumstances, under the authority of IRC 6103(p)(2)(B), an agreement may be created to allow for redisclosure of FTI. These agreements are negotiated and approved by the IRS Headquarters Office of Disclosure with concurrence of the Office of Safeguards.

Federal agencies authorized by statute to enter into redisclosure agreements are required to provide a copy of the executed agreement to the Office of Safeguards within thirty days of execution. The electronic copy must be emailed to the SafeguardReports@IRS.gov mailbox.

12.1 General

IRC Section 6103 authorizes the disclosure of FTI to specific federal agencies for use in statistical reports, for tax administration purposes, and certain other purposes specified in IRC Section 6103(j). 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 outside the agency 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.

12.2 Making a Request Under IRC Section 6103(j)

Federal agencies seeking statistical information from the 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.

12.3 State Tax Agency Statistical Analysis

State tax agencies who use FTI for tax administration purposes in tax modeling, revenue estimation or other statistical purposes must execute the Need and Use Justification statement once with subsequent updates to their statistical analysis activities updated annually in their SAR. (see sections 2.4 and 7.4.7)

The state tax agency should contact their servicing Disclosure Manager to secure the Need and Use Justification statement. The signed Justification statement must be returned to the local Disclosure Manager.

If the state agency utilizes a contractor to conduct the statistical analysis, tax modeling or revenue estimation, 45-day notification requirements apply. (see section 11.3)

12.4 Making a Request Under IRC Section 6108

State agencies seeking statistical information from the IRS should make their requests under IRC 6108 and address their request to the address specified in section 12.2 above. There is a charge for this data
.

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), (20) or (21) 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
(A) In general
The term “State” means—
(i) any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands,
(ii) 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, and
(iii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any governmental entity—
(I) which is formed and operated by a qualified group of municipalities, and
(II) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure.
(B) Regional income tax agencies
For purposes of subparagraph (A)(iii)—
(i) Qualified group of municipalities The term “qualified group of municipalities” means, with respect to any governmental entity, 2 or more municipalities—
(I) each of which imposes a tax on income or wages,
(II) each of which, under the authority of a State statute, administers the laws relating to the imposition of such taxes through such entity, and
(III) which collectively have a population in excess of 250,000 (as determined under the most recent decennial United States census data available).
(ii) References to State law, etc. For purposes of applying subparagraph (A)(iii) to the subsections referred to in such subparagraph, any reference in such subsections to State law, proceedings, or tax returns shall be treated as references to the law, proceedings, or tax returns, as the case may be, of the municipalities which form and operate the governmental entity referred to in such subparagraph.
(iii) Disclosure to contractors and other agents Notwithstanding any other provision of this section, no return or return information shall be disclosed to any contractor or other

agent of a governmental entity referred to in subparagraph (A)(iii) unless such entity, to the satisfaction of the Secretary—
(I) has requirements in effect which require each such contractor or other agent which would have access to returns or return information to provide safeguards (within the meaning of subsection (p)(4)) to protect the confidentiality of such returns or return information,
(II) agrees to conduct an on-site review every 3 years (or a mid-point review in the case of contracts or agreements of less than 3 years in duration) of each contractor or other agent to determine compliance with such requirements,
(III) submits the findings of the most recent review conducted under subclause (II) to the Secretary as part of the report required by subsection (p)(4)(E), and
(IV) certifies to the Secretary for the most recent annual period that such contractor or other agent is in compliance with all such requirements.
The certification required by subclause (IV) shall include the name and address of each contractor and other agent, a description of the contract or agreement with such contractor or other agent, and the duration of such contract or agreement. The requirements of this clause shall not apply to disclosures pursuant to subsection (n) for purposes of Federal tax administration and a rule similar to the rule of subsection (p)(8)(B) shall apply for purposes of this clause.
(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).

26 U.S.C. Section 6103(p)(4)

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), (20) or (21) 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).

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

(a) In general. Notwithstanding any section of the Internal Revenue Code (Code), the Internal Revenue Service (IRS) may terminate or suspend disclosure of returns and return information to any authorized recipient specified in section (p)(4) of section 6103, if the IRS determines 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 received by the authorized recipient (and its authorized contractors or agents, if any). The request 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 shall hold a conference with representatives of the authorized recipient, after which the Commissioner or Deputy Commissioner shall make a final determination with respect to the appeal.

(e) Effective/applicability date. This section applies 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 11, 2009.

NIST Moderate Risk Controls for Federal Information Systems are required for systems processing Federal Tax Information

Note: Missing or asterisked controls are not required for Publication 1075 compliance.
(F) Indicates that the control is only applicable for Federal Agencies.

SECURITY CONTROLS: 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: Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); Establishing conditions for group membership; Identifying authorized users of the information system and specifying access privileges; Requiring appropriate approvals for requests to establish accounts; Establishing, activating, modifying, disabling, and removing accounts; Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and Reviewing accounts [Assignment: organization-defined frequency].

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 organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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-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 documents allowed methods of remote access to the information system; Establishes usage restrictions and implementation guidance for each allowed remote access method; Monitors for unauthorized remote access to the information system; Authorizes remote access to the information system prior to connection; and Enforces requirements for remote connections to the information system.

AC-18 WIRELESS ACCESS
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, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: Access the information system from the external information systems; and receive, process, store, and/or transmit organization-controlled information using the external information systems.

*AC-22 PUBLICLY ACCESSIBLE CONTENT
Control: The organization designates individuals authorized to post information onto an organizational information system that is publicly accessible; Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

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 organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]; Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].

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 REVIEW, ANALYSIS, AND REPORTING
Control: The organization reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

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.

AU-12 AUDIT GENERATION
Control: The information system provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components]; Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION CLASS: MANAGEMENT

CA-1 SECURITY ASSESSMENT POLICY AND PROCEDURES
Control: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

CA-2 SECURITY ASSESSMENTS
Control: The organization develops a security assessment plan that describes the scope of the assessment including: Security controls and control enhancements under assessment;
Assessment procedures to be used to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities; Assesses the security controls in the information system [Assignment: organization-defined frequency] 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; Produces a security assessment report that documents the results of the assessment; and Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

CA-3 INFORMATION SYSTEM CONNECTIONS
Control: The organization authorizes all connections from the information system to other information systems outside of the authorization boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CA-5 PLAN OF ACTION AND MILESTONES
Control: The organization develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 SECURITY AUTHORIZATION: The organization authorizes 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 authorization.

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 under configuration control, a current baseline configuration of the information system.

CM-3 CONFIGURATION CHANGE CONTROL
Control: The organization determines the types of changes to the information system that are configuration controlled; Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; Documents approved configuration-controlled changes to the system; Retains and reviews records of configuration-controlled changes to the system; Audits activities associated with configuration-controlled changes to the system; and
Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-4 SECURITY IMPACT ANALYSIS
Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

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 establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; Implements the configuration settings; Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

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.

CM-9 CONFIGURATION MANAGEMENT PLAN
Control: The organization develops, documents, and implements a configuration management plan for the information system that: Addresses roles, responsibilities, and configuration management processes and procedures; Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

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. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and

Communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].

(F) 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-6 ALTERNATE STORAGE SITE
Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup.

CP-7 ALTERNATE PROCESSING SITE
Control: The organization establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable; and ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

*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 information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and Protects the confidentiality and integrity of backup information at the storage location.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, 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 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational 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 information system identifiers for users and devices by: Receiving authorization from a designated organizational official to assign a user or device identifier; Selecting an identifier that uniquely identifies an individual or device; Assigning the user identifier to the intended party or the device identifier to the intended device; Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and Disabling the user identifier after [Assignment: organization-defined time period of inactivity].

IA-5 AUTHENTICATOR MANAGEMENT
Control: The organization manages information system authenticators for users and devices by:
Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; Establishing initial authenticator content for authenticators defined by the organization; Ensuring that authenticators have sufficient strength of mechanism for their intended use; Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; Changing default content of authenticators upon information system installation;
Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; Protecting authenticator content from unauthorized disclosure and modification; and Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

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.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

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.

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.

IR-8 INCIDENT RESPONSE PLAN
Control: The organization develops an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability; Describes the structure and organization of the incident response capability; Provides a high-level approach for how the incident response capability fits into the overall organization; Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; Defines reportable incidents; Provides metrics for measuring

the incident response capability within the organization. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and Is reviewed and approved by designated officials within the organization; Distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]; Reviews the incident response plan [Assignment: organization-defined frequency]; Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and Communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements].

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, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

MA-4 NON-LOCAL MAINTENANCE
Control: The organization authorizes, monitors, and controls any non-locally 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-3 MEDIA MARKING
Control: The organization marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and Exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].

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 [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]; Maintains accountability for 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, release out of organizational control, 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-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM
Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

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. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessment.

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.

(F) 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 an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; Reviews risk assessment results [Assignment: organization-defined frequency]; and Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state 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 the following requirements and/or specifications, 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: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.

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-10 DEVELOPER CONFIGURATION MANAGEMENT
Control: The organization requires that information system developers/integrators: Perform configuration management during information system design, development, implementation, and operation; Manage and control changes to the information system;. Implement only organization-approved changes; Document approved changes to the information system; and Track security flaws and flaw resolution.

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 the network connection associated with a communications session at the end of the 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 DEVICES
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 provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address 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 internal/external role.

SC-23 SESSION AUTHENTICITY
Control: The information system provides mechanisms to protect the authenticity of communications sessions.

*SC-28 PROTECTION OF INFORMATION AT REST
Control: The information system protects the confidentiality and integrity of information at rest.

(F) SC-32 INFORMATION SYSTEM PARTITIONING
Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

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, ADVISORIES, AND DIRECTIVES
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.

(F) SI-7 SOFTWARE AND INFORMATION INTEGRITY
Control: The information system detects unauthorized changes to software and information.

SI-8 SPAM PROTECTION
Control: The organization employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

SI-9 INFORMATION INPUT RESTRICTIONS
Control: The organization restricts the capability to input information to the information system to authorized personnel.

SI-10 INFORMATION INPUT VALIDATION
Control: The information system checks the validity of information inputs.

SI-11 ERROR HANDLING
Control: The information system identifies potentially security-relevant error conditions; Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and reveals error messages only to authorized personnel.

FAMILY: PROGRAM MANAGEMENT CLASS: MANAGEMENT

*PM-1 INFORMATION SECURITY PROGRAM PLAN
Control: The organization develops, reviews, revises and disseminates an organization-wide information security program plan.

*PM-2 SENIOR INFORMATION SECURITY OFFICER
Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

*PM-3 INFORMATION SECURITY RESOURCES
Control: The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and Ensures that information security resources are available for expenditure as planned.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS
Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

*PM-5 INFORMATION SYSTEM INVENTORY
Control: The organization develops and maintains an inventory of its information systems.

*PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE
Control: The organization develops, monitors, and reports on the results of information security measures of performance.

*PM-7 ENTERPRISE ARCHITECTURE
Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

*PM-8 CRITICAL INFRASTRUCTURE PLAN
Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

*PM-9 RISK MANAGEMENT STRATEGY
Control: The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and implements that strategy consistently across the organization.

*PM-10 SECURITY AUTHORIZATION PROCESS
Control: The organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and Fully integrates the security authorization processes into an organization-wide risk management program.

*PM-11 MISSION/BUSINESS PROCESS DEFINITION
Control: The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and determines information protection needs arising from the defined mission/business processes.

EXHIBIT 5 SANCTIONS FOR UNAUTHORIZED DISCLOSURE

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 6 CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE

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 7 SAFEGUARDING CONTRACT LANGUAGE

The agency should include the Exhibit 7 language for either General Services or Technology Services, as appropriate and include the language below to the greatest extent possible, applicable to the specific situation.

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 performed under the supervision of the contractor or the contractor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is 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 and products will be given the same level of protection as required for the source material.

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) 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.

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

(7) (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 shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of

unauthorized disclosure. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-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 this contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 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 so 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.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

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.

CONTRACT LANGUAGE FOR TECHNOLOGY 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 receiving, 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.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

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.
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

Control No.	Password Management Guidance
	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

These controls must be implemented at both the application and system levels.

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 modification.
17	The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.

Within the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application.

Federal Security Standards

- 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)
- The Keyed-Hash Message Authentication Code (FIPS 198-1)

Industry Security Standards

- Digital Certificate (ANSI X5.09 v3)
- Public Key Cryptography Using Irreversible Algorithms (ANSI X9.30)
- Agreement of Symmetric Keys Using Discrete Logarithm Cryptography (ANSI X9.42)
- Extension to Public Key Certificates and Certificate Renovation List (ANSI X9.55)
- Enhanced Management Controls Using Digital Signatures and Attribute Certificates (ANSI X9.45)

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 11 DATA WAREHOUSE CONCEPTS & SECURITY REQUIREMENTS

Note: When an agency implements a data warehouse, the agency must provide written notification to the IRS Office of Safeguards, identifying the security controls, including FTI identification and auditing within the data warehouse. The written notification shall be sent to the SafeguardReports@IRS.gov mailbox at least 45 days before implementation. In addition, implementation of a data warehouse constitutes a significant change under section 7.1, triggering the requirement for the submission of a new SPR. (Section 5.3)

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 11 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 also applies to authorized representatives, agents or contractors with access to 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 authorized representatives, agents or contractors with access to 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

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

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 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. Through 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 purposes defined within Publication 1075. As part of the data warehouse, FTI data must retain its identity as FTI to the data element level (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.

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 aspect of the data warehouse is assessed for risk. 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.

The agency must develop policies and procedures to document all existing business processes. The agency must ensure that roles are identified for the organization and develop responsibilities for the 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.

The agency must 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 authorized users with a demonstrated "need to know" can query FTI data within the data warehouse.

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 the current revision of NIST SP 800-53. 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.

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 additional physical security controls for a data warehousing environment. However, the physical security requirements resident throughout Publication1075 do apply to the physical space hosting the data warehouse hardware.

Contingency Planning

On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. Agencies will ensure the data being provided is reliable.

Both incremental and special purpose data back-up procedures are required, combined with 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, the agency's contingency plan must 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 FTI is used and how FTI is queried or targeted by end users. Parts of the system containing FTI 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. The agency's incident reporting policy and procedures must cover the data warehousing environment as well.

Awareness & Training

The agency shall have a disclosure awareness 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. The web portal and 2-factor authentication requirements in Section 9 apply in a data warehouse environment.

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
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 by each unique user. 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.

Procedures for 45-day Notification of contractor access to FTI

Federal agencies, state tax agencies, and state child support enforcement agencies in the possession of FTI may use contractors, sometimes in limited circumstances. Human Services agencies may not provide FTI access to contractors. Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor, or at least 45 days prior to the disclosure of FTI, to ensure appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors.

To provide agency notification of intent to enter into an agreement to make disclosures of FTI to a contractor, submit a letter in electronic format, on agency letterhead over the head of agency's signature, to SafeguardReports@IRS.gov. Ensure the letter contains the following specific information:

- Name, address, phone number and email address of agency point of contact
- Name and address of contractor
- Contract number and date awarded
- Period contract covers, e.g. 2003-2008
- Type of service covered by the contract
- Number of contracted workers
- Name and description of agency program contractor will support
- Detailed description of the FTI to be disclosed to contractor
- Description of the work to be performed by the contractor, including phased timing, how the FTI will be accessed and how tasks may change throughout the different phases
- Procedures for agency oversight on contractor access, storage and destruction of FTI, disclosure awareness training, and incident reporting
- Location where work will be performed (contractor site or agency location) and how data will be secured if it is moved from the secure agency location
- Statement whether subcontractor(s) will have access to FTI
- Name(s) and address(es) of all subcontractor(s), if applicable
- Description of the FTI to be disclosed to the subcontractor(s)
- Description of the work to be performed by subcontractor(s)
- Location(s) where work will be performed by subcontractor(s) and how data will be secured if it is moved from a secure agency location
- Certification that contractor personnel accessing FTI and contractor information systems containing FTI are all located within the United States or territories as FTI is not allowed off-shore.

After receipt of an agency's request, the IRS will analyze the information provided to ensure the contractor access is authorized and consistent with all requirements, then IRS will send the agency a written acknowledgement, along with a reminder of the requirements associated with the contract. Agency disclosure personnel may wish to discuss local procedures with their procurement colleagues to ensure they are part of

the contract review process and the appropriate contract language is included from the beginning of the contract.

If the 45-day notification pertains to the use of contractors in conducting tax modeling, revenue estimation or other statistical purposes utilizing FTI, the agency must also submit a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data statement to the IRS Statistics of Income office for approval of the methodology. (see section 11.3)

The text of the following banner is recommended for use by the Office of Safeguards. A warning banner is required when accessing any application containing FTI.

WARNING

This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

These two banners are approved by the Department of Justice for sytems that have limited space for the warning banner:

WARNING! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

WARNING! THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES, AS WELL AS CIVIL PENALTIES.

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 orinformation 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.

CORRECTIVE ACTION PLAN (CAP): A report required to be filed twice each year detailing the agency's planned and completed actions to resolve findings identified during an IRS safeguard review.

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. The POA&M arises from agency conducted internal inspections and highlights corrections arising from the agency conducted internal inspection. (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.

Publication 1075 (Rev. 8-2010) Catalog Number 46937O
Department of the Treasury **Internal Revenue Service** www.irs.gov