IRS Office of Safeguards

Sample Safeguards Procedures Report (SPR)

September 30, 2008

Introduction

By providing a sample completed SPR based on a hypothetical system that receives, stores, process, or transmits FTI, agencies can reference what type of information is exactly needed to fulfill SPR reporting requirements. As a result, IRS Office of Safeguards is expected to receive higher quality and completed SPRs which in turn should produce more effective agency level security controls being implemented, and more effective evaluation of the Safeguarding Procedures documented in the SPRs.

The information contained in the “Agency SPR Content” column is hypothetical data for a hypothetical agency and represents the information that IRS Office of Safeguards expects to be provided by the agency regarding their procedures for safeguarding FTI. Agencies should use this sample as a guide when updating their Safeguards Procedure Report.

IRS Office of Safeguards – Sample Safeguards Procedures Report (SPR)

Dated:
Reviewed:

#	**Pub. 1075 Requirement Reference page 31 – 34**	**Agency SPR Content**	**Additional Information Needed to be Submitted by Agency** Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
		1. Responsible Officer(s)	
1.1	*Is the name, title, address, and telephone number of the agency official authorized to request Federal tax information from the IRS, the SSA, or other authorized agency documented?*	John Doe Tax Department Administrator Central Collection Department 11111 NE 55th Ave. Cleveland, OH 44113 123.123.1234 johndoe@state.us	
1.2	*Is the name, title, address, and telephone number of the agency official responsible for implementing the safeguard procedures documented?*	John Doe Tax Department Administrator Central Collection Department 11111 NE 55th Ave. Cleveland, OH 44113 123.123.1234 johndoe@state.us	
2. Location of the Data			

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
2.1	*Is an organizational chart or narrative description of the receiving agency, which includes all functions within the agency where FTI will be processed or maintained, documented?* ***Note:*** *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 agency departments that use FTI are: 1. Administration 2. Legal 3. Special Audit Departments. Special Auditors are the primary users of the FTI. The Legal Department prepares court cases when needed. The Administration department provides oversight for both departments. The Tax Administrator appoints all Special Auditors after review of their education and experience. Only Special Auditors and three Managers have access to the Special Audit area and the IRS Room. After appointment to Special Audit, employees are further trained and screened by the Special Audit Primary contact. Before gaining separate access to the IRS room, all Special Auditors must complete and sign a confidentiality agreement.	
3. Flow of the Data			

IRS Office of Safeguards – Sample Safeguards Procedures Report (SPR)

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
3.1	*Is there 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*	The agency currently analyzes returns and info from all zip codes in the state for underreporting or non-reporting of income, and this process will be expanded to include all agency member municipalities. A flow chart showing the flow of FTI information and Security Procedures are enclosed with this SPR. Narrative of the flow chart is provided here: At this time, FTI is received via secure data transport (SDT) leveraging Tumbleweed product. All data received is stored and maintained only in the IRS room. Data is downloaded to a free-standing workstation that is in a room with five levels of security (see 5.1 and PL2 for full description of building security). Security is broken down into both logical and physical security as follows: Logical Security: 1. Servers and hardware a. Firewalls b. IDS / HIDS / NIDS c. Routers d. Ports e. Services f. Protocols g. Patch Management	

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
3.2	*Is commingled or transcribed FTI data kept by the agency described and documented in the procedures?*	FTI Data that is received by the agency through the approved downloading process from the Internal Revenue Service's (IRS) FTI data "Mailbox", is logged when received and immediately inputted into the Revenue System. The documented FTI data moves through the various departments as seen in the attached Flow/Security Chart. FTI is commingled with other state data in the Revenue system. FTI is properly labeled, safeguarded, and identified as FTI when it is resident in systems that contain other agency data. Electronic FTI files follow a standard naming convention that identifies the file as containing FTI.	

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
3.3	*Is any data turned over to an agency contractor for processing fully disclosed and provided accurate accounting?*	The agency uses an outside contractor for software provided by the XYZ company. The XYZ vendor is the only outside vendor used for receipt, storage or use of FTI, and all processing of the data by XYZ is done on-site at the agency in the IRS room. Prior to this contractor or any of its employees having access to the FTI they must undergo a limited background check (LBI). They also must sign a non-disclosure agreement, confidentiality agreement, and sign that they have read our Rules of behavior (and will comply to its stipulations). The department will continue to work with the our contracting officers to ensure that the required IRS contract language is included in the contracts with these agencies as they come up for renewal, and that as changes are made to IRS Publication 1075, those changes are also incorporated into the contracts of each of the agencies that have access to federal tax information.	
4. System of Records			

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
4.1	*Is 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 Page 34 removable media) specified?* ***Note:*** *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.*	All records of requests for, receipt of and disposition of FTI are maintained on a permanent basis. They are scanned electronically and then backed up for indefinite retention. All tapes have been returned to IRS, other media are destroyed in-house and paper media are shredded.	
5. Secure Storage of the Data			

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
5.1	*Is a description of the security measures employed to provide secure storage for the data when it is not in current use documented?* *Note: Secure storage encompasses such considerations as locked files or containers, secured facilities, key or combination controls, offsite storage, and restricted areas.* ***For Federal Agencies**, it is requested that they submit a Vulnerability Assessment based on General Services Administration standards for their building(s) as it addresses physical security.*	We have a minimum of three layers of security. Security guards are positioned at the perimeter entrances into the building, card reader access is required to enter our interior doors, and the data is stored in locked file cabinets/containers. Our computers are password protected and when the computer is idled for 15 minutes, it will go to the sleep mode and require authentication for access. Our offsite storage site meets the two-barrier rule. Doors that do not require card reader access have high security key locks installed with access limited to cleared personnel. All employees are aware of the clean desk policy. A vulnerability assessment by the Federal Protective Service on 9/9/09. The building is classified as a GSA Level III facility. Now that data is downloaded from the IRS SDT site, the downloaded data is stored in a PGP-encrypted directory on a PC referred to as the IRS PC or it is downloaded directly to the IRS production server. When downloaded to PC, the encrypted receiving directory is protected by private key and pass-phrase. The downloaded data is then uploaded to the agency's	

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
6. Restricting Access to the Data			

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
6.1	*Is there a documented 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? This includes a description of:* • *How the information will be protected from unauthorized access when in use by the authorized recipient,* • *The physical barriers to unauthorized access (including the security features where FTI is used or processed), and* • *Systemic or procedural barriers.*	Access to FTI is limited to those individuals that are located in the newly created IRS Secured Area. All reporting, compiling, sorting of any data will be restricted to those individuals and any other authorized individuals. See 5.1 for information regarding building security and physical barriers to the IRS room. Special training is also performed prior to granting a member of personnel access to the FTI. When FTI are in use outside of the IRS room, the forms are kept in specially-marked red folders in the Special Audit area (which has limited access as described in 5.1). The folders are returned to the IRS room at break times and at the end of the day. Per IRS regulations, the returns are kept in locked containers. They can be used at your desk each day, but the batch must be returned to the locked cabinet each night. Long term storage of FTI is maintained in a secure off-site environment with limited key access with two barriers. An access log is maintained at this storage facility. Cases referred to our Legal Department are stored in a file cabinet with a locking bar and padlock. The cabinet is locked at all times when	

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
7. Disposal			

#	Pub. 1075 Requirement Reference page 31 – 34	Agency SPR Content	Additional Information Needed to be Submitted by Agency Note- information noted in red must be submitted in 30 days, information noted in blue describes additional information needed.
7.1	*Is a description of the method(s) of FTI disposal (when not returned to the IRS) documented?* ***Note:*** *The IRS will request a written report that documents the method of destruction and that the records were destroyed.*	All FTI received are documented in writing in binders kept in the IRS room. Any data destroyed or returned to IRS are also documented. Further, the agency has developed a policy concerning FTI disposal. This agency policy describes the requirements and procedures used when disposing of FTI, in the event that it is not returned to the IRS. Federal returns, return information in paper format and any Ad Hoc reports or imaging software copies of FTI data are shredded to shredded to effect 5/16 inch wide or smaller strips; microfilm and microfiche are shredded to effect a 1/35- inch by 3/8- inch strips. Magnetic tape containing FTI is not 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 is destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration. Whenever disk media leaves the physical or systemic control of the agency for maintenance, exchange, or other servicing, any FTI on it is destroyed by completely overwriting	

8. Computer Security			
8.1	Name and Address of Data Center: Name, telephone number, and e-mail address of Security Administrator or other IT contact at the Data Center: Is this facility shared by other State agencies? A brief description of FTI data flow within all automated information systems and networks that receive, process, store, or transmit FTI: Brief description of IT environment: 1-Mainframe: e.g. IBM/Unisys Operating System: e.g. zOS v1.7 Security Software: RACF No. of production LPARs with FTI: 2-UNIX/LINUX: Operating System: e.g. Solaris v2.8 No. of production Servers with FTI: e.g. 4 Operating System: e.g. Red Hat v5.6	Central Collection Department 11111 NE 55th Ave. Cleveland, OH 44113 John Doe Tax Department Administrator 123.123.1234 johndoe@state.us Jane Doe Security Administrator 123.123.1235 janedoe@state.us Facility is not shared with other agencies. The FTI data is received via secure transmission. The data is encrypted with the latest FIPS requirements. If the data is sent from within the agency, we utilize VPN. If the data is sent from the IRS (or other location); then it is encrypted and utilizes TCP/IP via SSL. TCP/IP provides capabilities such that if the data is sent incompletely, it will be resent (SYN-ACK). The data traverses via a known port. The data does not traverse using Telnet or other known ports with vulnerabilities. When the data is received, it is received in an email as a flat file and then the user who received the data then migrates	

	No. of production Servers with FTI: e.g. 2 3-Windows: Operating System: e.g. Windows 2003 No. of production Servers with FTI: e.g. 4 Operating System: e.g. Windows 2002 No. of production Servers with FTI: e.g. 1 4-Tumbleweed: Operating System: e.g. Windows 2003 (server/workstation) No. of production Servers with FTI: e.g. 1	the data to the database within our agency. End User Workstation: Windows XP Professional with one workstation with FTI UNIX Database Server: One UNIX production server with FTI is running HP-UX 11.23 OS. There is one LPAR with RACF as the security software. The mainframe is an IBM zo/s. User access has been dictated by the UID string. Currently we have 21 character places in the UID string. The string is as follows: 1st 7 strings – User ID 2nd 7 strings – Dept and sub-department assignments 3rd 7 strings – Authorizations within mainframe	

8.2	**MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: RISK ASSESSMENT**			
	RA1	**PUBLICATION 1075 GUIDANCE:** 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.	The IT Risk Assessment Policy developed in January 2008 details the procedures necessary to complete a risk assessment. Some of the areas covered in the Risk Assessment Policy include: System Categorization Threat identification Vulnerability Assessment Control Analysis Likelihood of risks Magnitude of risks Risk Mitigating Control Assessment and Recommendation	

	RA3	**PUBLICATION 1075 GUIDANCE:** 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	Risks may be physical, logical, environmental, as well as an array of other risk topics. Upon conducting the agency Risk Assessment, the identification of those vulnerabilities will become known, and as such, they will be assessed in terms of their risk and magnitude. These vulnerabilities will then be incorporated into the agency Risk Assessment in terms of the acceptable level of risk to the agency as a whole. The RA was first developed in March 2008 and per agency policy will be reviewed annually and updated at least every 3 years (or earlier if a major system change occurs). The risk assessment covered all platforms that receive, store, process, or transmit FTI as described in section 8.1 of the SPR. The assessment was conducted using NIST 800-30 methodology, in accordance with agency policy.	
	RA4	**PUBLICATION 1075 GUIDANCE:** 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	The Risk Assessment is updated at least every 3 years. The document is updated earlier if there is a significant event that occurred such as a new system upgrade, major release, etc. The updates incorporate the new risks posed to ensure that security controls within the environment are also updated to match against the new risks.	

	RA5	**PUBLICATION 1075 GUIDANCE:** Periodically, systems that contain FTI shall be scanned to identify vulnerabilities in the information system. The agency shall identify the timeframe on how often scans are conducted.	Systems are scanned for vulnerability on a quarterly basis using automated vulnerability scanning tools. The types of scans deployed utilize known software such as Nessus, Nmap, and ShieldsUp. The types of scans are non-intrusive and identify those common ports (ephemeral) and services that may be exposed to vulnerabilities. If any vulnerabilities are identified; they are tracked in a plan of action and milestones and rectified within a reasonable timeframe (given the severity of the issue).	

8.3	**MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: SECURITY PLANNING**			
	PL1	**PUBLICATION 1075 GUIDANCE:** 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.	The Security Planning Policy developed in January 2008 details the procedures necessary to facilitate implementing security planning controls such as security plans, and rules of behavior. Some of the areas covered in the Security Planning Policy include: System Security Planning Rules of Behavior Privacy Impact Security Activity Planning	
	PL2	**PUBLICATION 1075 GUIDANCE:** Agencies must develop, document, and establish a system security plan by describing the security requirements, current controls and planned controls, for protecting agency information systems and Federal tax information.	A security plan has been developed. that provides an overview of the security requirements for the system and a description of the management, operational and technical security controls that are in place or planned for meeting those requirements. The Security Plan was first developed in March 2008 and per agency policy will be reviewed annually and updated at least every 3 years (or earlier if a major system change occurs).	

	PL3	**PUBLICATION 1075 GUIDANCE:** The system security plan must be updated to account for significant changes in the security requirements, current controls and planned controls for protecting agency information systems and Federal tax information.	The agency Security Plan policy is updated at least every 3 years. The document is updated earlier if there is a significant event that occurred such as a new system upgrade, major release, etc. The updates incorporate the new system changes or controls posed to ensure that security controls within the environment are also updated to match against the environment	
	PL4	**PUBLICATION 1075 GUIDANCE:** 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.	As part of the Security Plan one of the appendices is a Rules of Behavior. This document lays the foundation for the allowable actions for each user on the system, and specifically related to FTI. This document is then signed by each person with access to the environment (including contractors, vendors, etc.), as evidence that they have read, understood and agree to the stipulations set forth in the Rules of Behavior.	

	PL6	**PUBLICATION 1075 GUIDANCE:** 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.	Prior to the migration of any change (hotfix, release, patch, upgrade, system change, etc.); or upcoming security assessment (e.g., state audit, Safeguard review, internal risk assessment) coordination is done between the IT department and the Tax division to inform the users of potential operational impact. If possible, security assessment activities that will have operational impact are performed during non-business hours to reduce impact to operations.	

8.4	**MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND SERVICES ACQUISITION**			
	SA1	**PUBLICATION 1075 GUIDANCE:** 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 System Services and Acquisition Policy developed in January 2008 details the procedures necessary to facilitate implementing system and services acquisition controls such as system documentation and system life cycle considerations. Some of the areas covered in the System and Services Acquisition Policy include: System Development Lifecycle Acquisition of System Components System Documentation Software Usage Security Engineering External Information Services Developer Security	

	SA2	**PUBLICATION 1075 GUIDANCE:** 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.	The agency's capital planning and investment control process provides for the necessary resources required to adequately protect its information systems. The agency's annual budget provides appropriate expenditure levels for: System contractual services System hardware and software capital outlay and supplies System hardware and software maintenance System security IT management and staffing Tax administration management and staffing The agency's building structure and related security features were designed specifically to ensure that an appropriate level of resources is allocated to the physical protection of FTI.	

	SA3	**PUBLICATION 1075 GUIDANCE:** Whenever information systems contain FTI, the agency manages the information system using a system development life cycle methodology that includes information security considerations.	The IT department has developed a detailed system development life cycle (SDLC) that includes security requirements at each milestone and life cycle phase. The initiation and development phase of the lifecycle includes security requirements definition, initial risk assessment and security engineering design. The implementation phase includes security testing and mitigation of risk. The operations and maintenance phase includes change management and ongoing risk assessments, and the disposal phase includes execution of system disposal in a secure manner. See attached IT System Development Life Cycle.	
	SA4	**PUBLICATION 1075 GUIDANCE:** 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 Information Technology Department (ITD) has developed the a document which deals specifically with the acquisition of new information systems or software. This document, of which a copy is attached, requires that all technological purchases must have IT approval. Prior to the selection of any technology hardware/software system, the requestor is required to complete an “Impact Analysis Form”. This form will ensure that all technology standards are maintained and that all security requirements are included in acquisition contracts.	

	SA5	**PUBLICATION 1075 GUIDANCE:** Whenever information systems contain FTI, the agency shall obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.	The agency's Security Policy specifically indicates that the information system is adequately documented and that the system documentation is protected as required and made available to authorized personnel. Documentation maintained includes the security plan, which describes the system's security features; the Security User's guide, which describes how to effectively use the system's security features and is focused on the end user; and the Security Administrator guide, which has information on configuring and installing security features.	
	SA6	**PUBLICATION 1075 GUIDANCE:** Whenever information systems contain FTI, the agency complies with software usage restrictions.	Only the Special Audit Primary contact and software vendor are allowed to access, download or update any software on the workstation.	
	SA7	**PUBLICATION 1075 GUIDANCE:** Whenever information systems contain FTI, the agency shall enforce explicit rules governing the installation of software by users.	No users have administrator rights to a PC or the network except for those administrators who have been approved as such. Installation of software is prohibited in policy and also prevented within the network where FTI resides.	

	SA8	**PUBLICATION 1075 GUIDANCE:** Whenever information systems contain FTI, the agency shall design and implement the information system using security engineering principles.	As changes occur, the test plans, test results, user acceptance testing, as well as approvals are documented and maintained. The security engineering principles applied are increased for those changes that contain FTI. The procedures are detailed in The agency SDLC policy, which has 2 sets of guidelines. The first is for non-FTI data and the 2nd is for changes involving FTI.	
	SA11	**PUBLICATION 1075 GUIDANCE:** The information system developers shall create a security test and evaluation plan, implement the plan, and document the results.	The agency develops a formalized security test and evaluation (ST&E) for each new change before implementing in the production environment. This is performed to ensure that the new changes will account for any vulnerabilities identified in the ST&E. Functional testing that occurs in the development process is utilized to the extent possible to test security features.	
8.5	**MANAGEMENT SECURITY CONTROLS CONTROL FAMILY: CERTIFICATION & ACCREDITATION (C&A)**			

	CA1	**PUBLICATION 1075 GUIDANCE:** The agency shall develop and update a policy that addresses the processes used to test, validate, and authorize the security controls used to protect FTI. While state and local agencies are not required to conduct a NIST compliant C&A, the agency shall accredit in writing that the security controls have been adequately implemented to protect FTI. The written accreditation constitutes the agency's acceptance of the security controls and associated risks. However for federal agencies that receive FTI, a NIST compliance C&A is required in accordance with FISMA.	The Accreditation Policy developed in January 2008 details the procedures necessary to used to test, validate, and authorize the security controls used to protect FTI. Some of the areas covered in the Accreditation Policy include: Security Assessments System Interconnections Security Certification Security Accreditation Plan of Action & Milestones Continuous Monitoring	

	CA2	**PUBLICATION 1075 GUIDANCE:** The agency shall conduct an assessment of the security controls in the information system, periodically but at least annually, to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This assessment shall complement the certification process to ensure that periodically the controls are validated as being operational.	The security controls are tested at least annually for any system containing FTI. Should there be significant modifications or changes to that particular system; the testing will occur earlier. The testing is to ensure that there are no major vulnerabilities exposing the agency to increased risk with regard to the FTI data.	
	CA3	**PUBLICATION 1075 GUIDANCE:** 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 has a detailed network diagram, data flow diagram, as well as a network topology. These documents help to identify the various boundaries of scope. All connections are clearly marked in the diagrams. Any system that falls outside the boundary, but interfaces with a system inside the boundary contains a system connection agreement. This is to ensure that controls outside the boundary are the same or better for those systems interfacing with a system inside the boundary.	

	CA4	**PUBLICATION 1075 GUIDANCE:** 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.	Prior to any system being placed in the production environment, the system is assessed in terms of risk via a vulnerability assessment. Those weaknesses found are then mitigated or accepted so that the overall risk is at an acceptable level. The final determination of accreditation is a signature from The designated accrediting official. This serves as evidence that the system was assessed prior to being placed in production.	
	CA 5	**PUBLICATION 1075 GUIDANCE:** As recipients of FTI, the agency is responsible to develop and update a Plan of Action and Milestones (POA&M) that shall identify any deficiencies related to FTI processing. The POA&M shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during the review processes, either internal or external. The POAM shall address implementation of security controls to reduce or eliminate known vulnerabilities in the system.	As noted above, a formal risk assessment is performed at least annually. Should there be any vulnerabilities identified that require remediation; they are detailed on a formal POA&M. The POA&M is a formal document for tracking the remaining items to be remediated. This document is critical, because without it; there will be issues not fully remediated; thus exposing the agency to risk with regard to the FTI data.	

	CA 6	**PUBLICATION 1075 GUIDANCE:** Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security accreditation. All information regarding the accreditation shall be provided to the Office of Safeguards as part of the Safeguard Activity Report.	The accreditation of systems occurs every 3 years or earlier if a significant event warrants the change (e.g. major upgrade, or release). The agency has appointed a formal designated accrediting official (DAA), which has been given responsibility for signing off indicating that the accreditation is in place.	
	CA7	**PUBLICATION 1075 GUIDANCE:** 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.	The DAA assigns monitoring duties over the control structure to ensure that controls are still in place and operating effectively. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting.	
8.6	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: PERSONNEL SECURITY**			

	PS1	**PUBLICATION 1075 GUIDANCE:** 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.	The Personnel Security Policy developed in January 2008 details the procedures necessary to facilitate implementing personnel security controls. The policy details specific requirements necessary for an employee to be granted access to FTI. Some of the areas covered in the Personnel Security Policy include: Position Categorization Personnel Screening Personnel Termination/Transfer Access Agreements Third-Party Personnel Security Personnel Sanctions	
	PS2	**PUBLICATION 1075 GUIDANCE:** Agencies must assign risk designations to all positions and establish screening criteria for individuals filling those positions.	All positions are assigned to specific risk designations. Depending on those risk designations and positions; the criteria for filling that position will vary. For example, security administrators with access to FTI will require a more extensive background check than will a non-FTI position. These policies are contained in the Personnel Security Policy.	

	PS3	**PUBLICATION 1075 GUIDANCE:** Individuals must be screened before authorizing access to information systems and information.	Any person wishing to access a system (whether it contains FTI or not) must undergo a background investigation and be properly screened. The screening must be positive and the results must have a signature from a member of The security team indicating that the person is permitted to have access to the systems. An additional layer of screening is included for individuals being considered for access to FTI.	
	PS4	**PUBLICATION 1075 GUIDANCE:** Agencies must terminate information system access, conduct exit interviews, and ensure return of all information system-related property when employment is terminated.	Within The agency, Information Technology and HR work closely together. Immediately after a person has been terminated notification is sent to IT at which time the person's system access is revoked immediately. Information system-related property is collected from the employee upon their departure, This property may include keys, identification cards, and building passes. The timely execution an employee termination is dependent on the type of departure the person had. For example, if the termination was unfriendly, then the termination is immediate. If the termination is friendly with the employee giving 2 weeks notice the employee may have limited access during that period. The details are specified in the Personnel Security Policy.	

	PS5	**PUBLICATION 1075 GUIDANCE:** Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.	Prior to any user gaining access to the systems; they must complete an access authorization form. This form is used to request access based on that user's job description. The user's supervisor approves the access and then forwards the request to IT so that the access can be granted within the system. If a user changes positions, gets promoted, etc., then HR notifies IT immediately. The system administrators will then contact the person's supervisor and ensure that system accounts and privileges are removed.	
	PS6	**PUBLICATION 1075 GUIDANCE:** Appropriate access agreements must be completed before authorizing access to users requiring access to the information system and Federal Tax Information.	The agency has instructed the various Departments that they will need to ensure that all personnel, before being granted access to the agency's technology, sign the access authorization document and comply with the terms of the administrative regulation, including terms of access to FTI and potential penalties of an unauthorized disclosure.	
	PS7	**PUBLICATION 1075 GUIDANCE:** Personnel security requirements must be established for third-party providers and monitored for provider compliance.	Third party providers are not used for The agency; however should we decide to use them in the future they will be required to undergo and adhere to the same restrictions and rules as The employees.	

	PS8	**PUBLICATION 1075 GUIDANCE:** Agencies must also establish a formal sanctions process for personnel who fail to comply with established information security policies, as this relates to FTI.	Violators of the policies and procedures referenced above are subject to disciplinary measures including privilege revocation and/or employment termination. In addition, the formal sanctions process used by Personnel Security and Human Resources includes penalties for unauthorized disclosure of FTI.	
8.7	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: CONTINGENCY PLANNING**			

	CP1 CP2	**PUBLICATION 1075 GUIDANCE:** 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.	The Contingency Policy developed in January 2008 details the procedures necessary to facilitate retrieving FTI data in the event of a system disruption or disaster. Some of the areas covered in the Contingency Planning Policy include: Contingency Plan Development Contingency Training Contingency Test/Exercises Off-Site Storage Alternate Processing Site System Backups System Recovery Procedures The Information Technology Department has a documented Disaster Recovery Plan.	

	CP4	**PUBLICATION 1075 GUIDANCE:** 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.	The Agency Contingency Plan is tested fully every 3 years and in a limited capacity every year. Further, if there are significant events that occur during the year such as a major upgrade, then the Contingency Plan would be tested earlier. Part of the testing process involves the use of restoring data from backup as well as incorporating use of the alternate sites.	
	CP6	**PUBLICATION 1075 GUIDANCE:** Agencies must identify alternate storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups.	The agency uses an alternate site. We have agreements in place to ensure that they adhere to specific requirements concerning the FTI. The data at the external site is segregated from other agencies and companies. The data is encrypted and password protected; thus personnel at the backup site cannot view the data.	
	CP7	**PUBLICATION 1075 GUIDANCE:** 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.	The Contingency Plan details alternate processing sites. We have agreements in place with an alternate site that acts as a hot site. There are specific parameters in place governing the confidentiality, integrity and availability over the FTI data. Should there be a need to resume operations from the alternate site, one of the personnel members must be present to ensure the protection of the FTI.	
8.8	**OPERATIONAL SECURITY CONTROLS**			

	CONTROL FAMILY: CONFIGURATION MANAGEMENT			
	CM1	**PUBLICATION 1075 GUIDANCE:** Configuration management policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing configuration management security controls.	The Configuration Management policy developed in January 2008 details the procedures necessary to facilitate implementing configuration management controls. Some of the areas covered in the Configuration Management Policy include: Configuration Change Control Monitoring Configuration Changes Access Restrictions for Change Secure Configuration Settings Least Functionality System Inventory	
	CM2	**PUBLICATION 1075 GUIDANCE:** The organization develops, documents, and maintains a current baseline configuration of the information system.	The agency has and maintains a baseline configuration of each system containing FTI that includes the standard software load and patch information. If there are changes that are made to the system then the baseline is updated accordingly. The agency has a history of baselines so that we can trace each change to the baseline.	
	CM3	**PUBLICATION 1075 GUIDANCE:** Authorize, document, and control changes to the information system.	Changes to the information system are managed using the agency's configuration management process outlined in the attached Configuration Management plan. The process includes documenting changes in a standard form Z1A-5, the steps for	

			obtaining approval through the IT Configuration Control Board, and testing changes prior to implementation.	
	CM4	**PUBLICATION 1075 GUIDANCE:** Monitor changes to the information system conducting security impact analysis to determine the effects of the changes.	To be consistent with the SDLC and the Configuration Management Policy, all changes are assessed in terms of their security impact. Should a change pose a security impact that is creates a significant vulnerability to the FTI data; then the change may not occur. Each change is assessed and a determination is made and signed off for evidence of a security impact analysis.	
	CM5	**PUBLICATION 1075 GUIDANCE:** 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.	The agency has 3 environments. They are development, test, and production. There are users with access to both development and test, but a second set of users with access to production. No user has access to all 3 environments. All access is reviewed prior to gaining access to the systems and access is then reviewed periodically as part of the access recertification process.	
	CM6	**PUBLICATION 1075 GUIDANCE:** 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	Mandatory configuration settings are deployed for those systems housing FTI. Those settings are the most restrictive regarding user authorizations. Those configuration settings are documented in the Configuration Management Policy and they are enforced via IT. Mandatory configuration settings are based on the technology specific security	

		consistent with operational requirement; (ii) documents the configuration settings; and (iii) enforces the configuration settings in all components of the information system.	configuration checklists published by the NIST Checklist Program.	
	CM7	**PUBLICATION 1075 GUIDANCE:** 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. Configure the information system to provide only essential capabilities. Prohibit the use of functions, ports, protocols, and services not required to perform essential capabilities for processing, storing, or transmitting Federal tax information.	As agency policy, systems are configured to only provide the minimum services necessary for operation. Information technology publishes a list of vulnerable ports and services that should be disabled. Access restrictions are deployed to ensure integrity and confidentiality over FTI data are maintained.	
	CM8	**PUBLICATION 1075 GUIDANCE:** Develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.	A complete listing of the system hardware and software components are maintained and updated whenever there is a change. This inventory listing is maintained in a secure library with restricted access to that library.	
8.9	**OPERATIONAL SECURITY CONTROLS**			

	CONTROL FAMILY: MAINTENANCE			
	MA1	**PUBLICATION 1075 GUIDANCE:** 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.	The agency, through its Information Technology department has developed, documented, disseminated and continuously updates the maintenance controls associated with the agency's information systems. The System Maintenance policy developed in January 2008 details the procedures necessary to facilitate implementing maintenance security controls. Some of the areas covered in the System Maintenance Policy include: System Maintenance Procedures Approved Maintenance Tools Remote Maintenance Maintenance Personnel It is imperative that the network remain available for us to continue operations. As such, the network must undergo routine maintenance such as hot fixes, patch updates, new security updates, etc. Files must be purged to relieve the network of clogging. There are also other procedures in place and they are documented in the Maintenance Policy, along with the tools deployed to maintain the network.	
	MA2	**PUBLICATION 1075 GUIDANCE:** The agency must ensure that	Maintenance is performed on a routine basis via software tools that identify CPU usage, space availability,	

		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.	etc. The Information Technology Department has developed a series of scheduled updates and maintenance to all agency owned equipment. A sample of the maintenance to desktops is as follows: “Anti Virus software is loaded on all desktops and laptops. Automated updates will ensure that the software is always current. Approved Microsoft updates and patches for critical security vulnerabilities are loaded as soon as they are released by Microsoft”	
	MA3 MA4	**PUBLICATION 1075 GUIDANCE:** Agencies must approve, control, and routinely monitor the use of information system maintenance tools and remotely-executed maintenance and diagnostic activities.	The tools deployed are also reviewed to ensure the agency is using the tools that will not introduce vulnerabilities into the environment. As such, the agency has a formal procedure in place for approving software maintenance tools.	
	MA5	**PUBLICATION 1075 GUIDANCE:** The agency allows only authorized personnel to perform maintenance on the information system.	Vendor support technicians must be authorized before they are granted access to the system for maintenance work. All support technicians that will have access to systems containing FTI undergo background checks initiated by Personnel Security and Human Resources.	
8.10	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND INFORMATION INTEGRITY**			

	SI1	**PUBLICATION 1075 GUIDANCE:** System and information integrity policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing system and information integrity security controls. Such system and information integrity security controls include flaw remediation, intrusion detection tools and techniques, information input restrictions, and information output handling and retention.	The System and Information Integrity policy developed in January 2008 details the procedures necessary to facilitate implementing system and information integrity controls, including flaw remediation, intrusion detection and output handling. Some of the areas covered in the System and Information Integrity Policy include: Flaw Remediation Anti-Virus Spam Protection System Input Restrictions System Error Handling System Output Handling	
	SI2	**PUBLICATION 1075 GUIDANCE:** Agencies must identify, report, and correct information system flaws.	As flaws are identified From various sources including the help desk from end user feedback, vendor web sites and mailing lists, and security assessments. Newly released security patches, service packs, and hot fixes are tested for effectiveness and potential side effects on the information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously.	
	SI3	**PUBLICATION 1075 GUIDANCE:**	All of the IT systems, including those systems containing FTI, are provided	

		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.	with McAfee anti-virus software with automatic scanning and automated virus definition updates.	
	SI4	**PUBLICATION 1075 GUIDANCE:** Intrusion detection tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of the information system and FTI.	The agency network contains both network and host based intrusion detection systems to identify potential intrusions on the network and the server itself and detect vulnerabilities, changes to the network, both known and unknown attack signatures, and traffic anomalies. The firewall also logs all traffic coming into the network.	
	SI5	**PUBLICATION 1075 GUIDANCE:** The agency shall receive and review information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	The IT department reviews vendor web sites, mailing lists, third party web sites, mailing lists and newsgroups, and vulnerability databases on a periodic basis from known and reputable sites such as SANS and CERT. The alerts are reviewed to ascertain if the security posture should be modified.	
	SI9	**PUBLICATION 1075 GUIDANCE:** Agencies must restrict information system input to authorized personnel (or processes acting on behalf of such personnel) responsible for processing, storing, or transmitting FTI.	All input into information systems is restricted to authorized personnel only. In order for an employee to get authorization to a system they must complete the access authorization form, which lists the systems to be accessed as well as the level of access. This access is then reviewed and approved by a supervisor and subsequently recertified with the periodic access recertification.	
	SI12	**PUBLICATION 1075**	Information is output from system on	

		GUIDANCE: Agencies must handle and retain output from the information system, as necessary to document that specific actions have been taken.	screen, to the hard drive via a file download or to the printer for a hard copy report. Each form of output is handled in accordance with agency security policies discussed in previous sections of this document.	
8.11	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: INCIDENT RESPONSE**			
	IR1	**PUBLICATION 1075** **GUIDANCE:** Incident response policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate the implementing incident response security controls. Such incident response security controls include incident response training and incident reporting and monitoring.	The Incident Response policy developed in January 2008 details the procedures necessary to facilitate responding to IT security incidents. Some of the areas covered in the Incident Response Policy include: Incident Handling Procedures Incident Reporting Procedures Incident Response Training Incident Response Test/Exercise	
	IR2	**PUBLICATION 1075** **GUIDANCE:** Agencies must train personnel in their incident response roles on the information system and FTI. Incident response training must provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication, and recovery.	As part of the annual security awareness training, all personnel are trained to handle and report various types of incidents. For example, if an employee receives a call asking for a password users are trained to not give that data over the telephone at all and to contact the computer security incident response team. If someone receives an email that looks like spam and it contains an attachment, users are trained to not open the email and to contact the computer security incident response team.	

	IR3	**PUBLICATION 1075 GUIDANCE:** The agency shall test and/or exercise the incident response capability for the information system at least annually to determine the incident response effectiveness and documents the results.	Exercises are performed annually against the agency's incident response procedures. This is performed in two ways. First, social engineering techniques are deployed against our employees to ascertain if they reveal information that shouldn't be revealed. The second form of testing is a scenario-based exercise of an incident in which employees are to respond as if a real incident has occurred.	
	IR5	**PUBLICATION 1075 GUIDANCE:** Agencies must routinely track and document information system security incidents potentially affecting the confidentiality of FTI.	The computer security incident response team implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Lessons learned from ongoing incident handling activities are incorporated into the incident response procedures the procedures are implemented accordingly. All incidents are tracked and monitored for resolution.	
	IR6	**PUBLICATION 1075 GUIDANCE:** Any time there is a compromise to FTI, the agency promptly reports incident information to the appropriate Agent-in-Charge, TIGTA.	For incidents involving the unauthorized disclosure or inspection of FTI, the Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) is promptly notified.	
	IR7	**PUBLICATION 1075 GUIDANCE:** The agency shall also provide an incident response support	The computer security incident response team is required to be a highly skilled and available group. Members of the team must meet at	

		resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability.	least once a month to establish and maintain incident procedures, classifications, and contact information.	
8.12	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: SECURITY AWARENESS AND TRAINING**			
	AT1	**PUBLICATION 1075 GUIDANCE:** 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.	The Security Awareness and Training policy developed in January 2008 details the procedures necessary to facilitate security awareness and training of agency employees. Some of the areas covered in the Security Awareness and Training Policy include: Security Awareness Program Security Training Security Training Records	
	AT2	**PUBLICATION 1075 GUIDANCE:** Agencies must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to the system.	Prior to gaining access to any system, all users must undergo training as part of their 'on boarding' process. They must also sign that they have taken the training.	
	AT3	**PUBLICATION 1075 GUIDANCE:** Agencies must identify personnel with significant information	An additional layer of training is provided for those personnel in IT security as well as for those with access to any FTI. This is also	

		system security roles and responsibilities, document those roles and responsibilities and provide sufficient security training before authorizing access to the information system and FTI.	required prior to those personnel gaining access to the systems.	
	AT4	**PUBLICATION 1075 GUIDANCE:** Agencies must document and monitor individual information system security training activities including basic security awareness training and specific information system security training.	All training evidence is maintained by the agency's learning and Education Coordinator. Personnel must sign when they take training. The sign-in sheets are then scanned and maintained electronically.	
8.13	**OPERATIONAL SECURITY CONTROLS CONTROL FAMILY: MEDIA ACCESS PROTECTION**			
	MP1	**PUBLICATION 1075 GUIDANCE:** 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.	The Media Protection policy developed in January 2008 details the procedures necessary to facilitate protection of data stored on various types of media. Some of the areas covered in the Media Protection Policy include: Media Access Restrictions Media Storage Media Transport Media Sanitization and Disposal	
	MP2	**PUBLICATION 1075 GUIDANCE:** The agency shall restrict access to information system media to	The Media Protection policy prevents FTI from being downloaded to USB drives, flash drives, removable hard drives, CDs and DVDs. FTI is	

		authorized individuals, where this media contains FTI.	sometimes printed in hard copy reports, and those reports are covered when transported and locked in a secure container in the office when not in use.	
	MP4	**PUBLICATION 1075 GUIDANCE:** The agency will physically control and securely store information system media within controlled areas, where this media contains FTI.	Servers that contain FTI are housed in a secure computer room that is restricted to authorized personnel only.	
	MP5	**PUBLICATION 1075 GUIDANCE:** All media being transmitted from the IRS must employ the use of encryption.	All transmissions of FTI from the IRS use Tumbleweed Secure Transport Client with an IdenTrust Aces Business Certificate. This transmission is over an SSL connection to/from the IRS SDT Server.	
	MP6	**PUBLICATION 1075 GUIDANCE:** The agency shall sanitize information system media prior to disposal or release for reuse.	In the past, when magnetic tapes received from the IRS were to be destroyed, they were first degaussed and then drilled several times before they were shredded. Backup tapes are encrypted and Veritas Barcode rules are used to ensure that IRS tapes are only reused as IRS tapes. Failed, broken and/or outdated tapes are subject to degaussing and shredding.	
8.14	**TECHNICAL SECURITY CONTROLS CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION**			
	IA1	**PUBLICATION 1075 GUIDANCE:**	The Identification and Authentication policy developed in January 2008	

		Identification and authentication policy and procedures must be developed, documented, disseminated, and updated, as necessary, to facilitate implementing identification and authentication security controls.	details the procedures necessary to facilitate user identification and authentication, such as username and password controls. Some of the areas covered in the Identification and Authentication Policy include: User Identification and Authentication Mechanism User ID Management Password Management	
	IA2 IA3	**PUBLICATION 1075 GUIDANCE:** 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.	Passwords are used as a standard authentication method and each user is assigned a unique ID. Tokens, smart cards or biometrics are not used at this time.	
	IA4	**PUBLICATION 1075 GUIDANCE:** 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;	A supervisor has to submit a request to the IT Department Help Desk to initiate a ticket for a Systems Administrator to create/disable/terminate user account and privileges. If a system account is locked or disabled due to too many login attempts or inactivity a user has to submit a request to the DOT Help Desk to initiate a ticket to reinstate	

		(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.	user account privileges. All requests are documented by the CA Unicenter Service Desk application used by the DOT Help Desk.	
	IA6	**PUBLICATION 1075 GUIDANCE:** The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Passwords are obscured when the user keys them into the system. Additionally, the error message displayed on screen when authentication fails does not provide information that could lead to exploitation.	
	IA7	**PUBLICATION 1075 GUIDANCE:** Whenever agencies are employing cryptographic modules, the agency shall work to ensure these modules are compliant with NIST guidance, including FIPS 140-2 compliance.	Agency employs cryptographic modules in Hummingbird Exceed 2008 and Hummingbird Connectivity Secure Shell 2008 that are FIPS 140-2 compliant.	
8.15	**TECHNICAL SECURITY CONTROLS CONTROL FAMILY: ACCESS CONTROL**			
	AC1	**PUBLICATION 1075 GUIDANCE:** Access control policy and procedures must be developed, documented, disseminated, and	The Access Control policy developed in January 2008 details the procedures necessary to facilitate access controls to the systems, such as , limiting access to those with a	

		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.	need-to-know, information-flow enforcement, and separation of duties, least privilege. Some of the areas covered in the Access Control Policy include: Account Management System Permissions Separation of Duties Role Based Access Control System Warning Banner Session Controls Remote Access	
	AC2	**PUBLICATION 1075 GUIDANCE:** Agencies must manage information system user accounts, including establishing, activating, changing, reviewing, disabling, and removing user accounts.	Windows Domain users are managed when they become inactive. A 45 day report is sent to the Windows Administrator who then runs a script which will disable any inactive user. If the domain user needs the account reactivated they request this from the help desk then the user is verified and a ticket to re-enable the account is sent to the System Administrator. Based on the Help Desk requests, the system Administrators manage server accounts including establishing, activating, disabling, reviewing, and removing. User access is reviewed for appropriateness every quarterly as part of the access recertification procedures.	

	AC3 AC4	**PUBLICATION 1075** **GUIDANCE:** The information system must enforce assigned authorizations for controlling system access and the flow of information within the system and between interconnected systems.	Access to the server is enforced by enabled TCP wrappers that use access control files (hosts.allow and hosts.deny). The access control files are being reviewed on an ongoing basis.	
	AC5	**PUBLICATION 1075** **GUIDANCE:** Agencies must ensure the information system enforces separation of duties through assigned access authorizations.	Separation of duties is enforced by access authorizations. For an example "oracle" account does not have a super user privileges. Users are included in groups with access restricted to selected applications and read-only access to data files.	
	AC6	**PUBLICATION 1075** **GUIDANCE:** The information system must enforce the most restrictive access capabilities users need (or processes acting on behalf of users) to perform specified tasks.	As user access is approved and granted; the most restrictive access is given in terms of the concept of least privilege. No user is given more rights than they require to do their job.	
	AC7	**PUBLICATION 1075** **GUIDANCE:** 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.	After 3 consecutive failed logon attempts, the user account is locked and must contact the Help desk to have the password reset.	
	AC8	**PUBLICATION 1075** **GUIDANCE:**	The IRS approved banner is configured for all services that allow	

		The information system must display an approved system usage notification before granting system access informing potential users that (i) the system contains U.S. Government information; (ii) users actions are monitored and audited; and (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties. Policy must be enforced so that a workstation and/or application are locked after a pre-defined period. This will ensure that unauthorized staff or staff without a need-to-know cannot access FTI.	login access to the server and FTI.	
	AC12	**PUBLICATION 1075 GUIDANCE:** 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.	Remote sessions are automatically terminated after a period of 15 minutes of inactivity.	
	AC13	**PUBLICATION 1075 GUIDANCE:** Management must supervise and review the activities of the users as this relates to information system access.	Access reviews occur upon initial granting of the access as well as periodically as part of the access recertification process.	
	AC14	**PUBLICATION 1075 GUIDANCE:**	There is no user action that can be performed on the information system	

		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.	that does not require authentication or identification. The Tax Division's public web site does not interface with the Tax database or any FTI data.	
	AC17	**PUBLICATION 1075 GUIDANCE:** Agencies must authorize, document, and monitor all remote access capabilities used on the system, where these systems containing FTI.	All remote access is controlled through the agency's enterprise VPN solution.	
	AC18	**PUBLICATION 1075 GUIDANCE:** Agencies must develop policies for any allowed wireless access, where these systems contain FTI. As part of the wireless access, the agency shall authorize, document, and monitor all wireless access to the information system.	There is no wireless access into the Tax database or FTI database. Wireless networks have been disabled. They have proven to be too dangerous for transmissions of data and as such we do not deploy wireless access points.	
	AC19	**PUBLICATION 1075 GUIDANCE:** Agencies must develop policies for any allowed portable and mobile devices, where these systems contain FTI. As part of this, the agency shall authorize,	The policy is that no FTI is allowed to be stored on any portable and mobile device such as laptop or PDA.	

		document, and monitor all device access to organizational information systems.		
	AC20	**PUBLICATION 1075 GUIDANCE:** Agencies must develop policies for authorized individuals to access the information systems from an external system, such as access allowed from an alternate work site. This policy shall address the authorizations allowed to transmit, store, and/or process FTI. As part of this, the agency shall authorize, document, and monitor all access to organizational information systems, where these systems contain FTI.	The policy is that Tax Data can only be accessed from the regular work site of the Division or the Data Center's offices.	
8.16	**TECHNICAL SECURITY CONTROLS CONTROL FAMILY: AUDIT AND ACCOUNTABILITY**			
	AU1	**PUBLICATION 1075 GUIDANCE:** 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	The Audit and Accountability policy developed in January 2008 details the procedures necessary to facilitate auditing of actions taken on the systems. Some of the areas covered in the Audit and Accountability Policy include: Security Event Auditing Audit Log Storage Audit Log Monitoring Audit Report Generation	

		monitoring, analysis and reporting; time stamps; protecting audit information and audit retention.	Audit Record Retention	
	AU2	**PUBLICATION 1075 GUIDANCE:** 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.	The system is configured to audit all administrative, privileged and security actions and discretionary access control permissions modifications. Audit logs are captured at both the UNIX and Windows operating system, as well as on the Revenue application itself and the supporting Oracle database. Audit records are also maintained in the mainframe (RACF security). Each event or object that is triggered, creates a SMF record. The database residing on the mainframe is an Oracle database. The Oracle database security is captured within the RACF security application. The operating system (MVS) controls are also captured within the RACF security package.	
	AU3	**PUBLICATION 1075 GUIDANCE:** 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	Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.	

		application-level events. Audit logs must enable tracking activities taking place on the system.		
	AU4	**PUBLICATION 1075 GUIDANCE:** Agencies must configure the information system to allocate sufficient audit record storage capacity to record all necessary auditable items.	Audit log sizes are set within the server. The server has several options such as size limits, overwrite, or save to disk. Currently the server is set to disk so that when it gets full the data is automatically transferred to another medium.	
	AU5	**PUBLICATION 1075 GUIDANCE:** The information system shall alert appropriate organizational officials in the event of an audit processing failure and takes the additional actions.	In the event that the server is not working correctly and the audit process causes an error; the server automatically sends an email alert to the system administrators.	
	AU6	**PUBLICATION 1075 GUIDANCE:** 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.	In addition to the internal reviews of FTI accesses, the Division Administrator and Sec Manager Tax (Assistant Administrator) receive and review a daily report which shows all suspicious activity regarding tax accounts.	
	AU7	**PUBLICATION 1075 GUIDANCE:** To enable review of audit records, the information system provides an audit reduction and report generation capability.	The audit settings are set such that filters are in place to reduce the logs so that only those items that are important appear on the logs.	
	AU8	**PUBLICATION 1075 GUIDANCE:** The information system shall provide date and time stamps for	All audit records provide time and date stamps of when the incident occurred. The audit logs are also tied to the time server.	

		use in audit record generation.		
	AU9	**PUBLICATION 1075 GUIDANCE:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The audit logs are only viewable by authorized system administrators. Only the security administrator has the system privilege to modify the audit log contents.	
	AU11	**PUBLICATION 1075 GUIDANCE:** 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.	All audit information is placed on a separate medium (e.g. disk) and backup as part of the weekly backup off-site storage process. Currently, this is retained for 7 years.	
8.17	**TECHNICAL SECURITY CONTROLS CONTROL FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION**			
	SC1	**PUBLICATION 1075 GUIDANCE:** System and communications policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing effective system and communications.	The System and Communications Protection policy developed in January 2008 details the procedures necessary to facilitate secure system communications. Some of the areas covered in the System and Communications Protection Policy include: System Partitioning Object Reuse Denial of Service Protection System Boundary Protection Data Transmissions Encryption	

	SC2	**PUBLICATION 1075 GUIDANCE:** The information system shall separate front end interface from the back end processing and data storage.	Front end processing is separate from back end processing. They are not only separate physically but also logically. End users do not have any access to the back end processing.	
	SC4	**PUBLICATION 1075 GUIDANCE:** The information system shall prevent unauthorized and unintended information transfer via shared system resources.	There are no shared resources. The data resides in a dedicated server in a dedicated Oracle database.	
	SC7	**PUBLICATION 1075 GUIDANCE:** 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.	All systems are monitored at the perimeter of the network. The agency's intrusion detection systems monitor the traffic and the payload.	
	SC9	**PUBLICATION 1075 GUIDANCE:** The information system must protect the confidentiality of FTI during electronic transmission.	The confidentiality of the data is protected via the VPN as data traverses. The data is also encrypted which protects against data confidentiality.	
	SC10	**PUBLICATION 1075 GUIDANCE:** 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.	After a period of inactivity (currently set to 15 minutes); the session is automatically set to terminate.	
	SC12	**PUBLICATION 1075 GUIDANCE:**	The agency deploys a server that also has CA capabilities. For those areas	

		When Public Key Infrastructure (PKI) is used, the agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	where PKI is deployed, our agency also manages the keys.	
	SC13	**PUBLICATION 1075 GUIDANCE:** 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 encryption is deployed, it utilizes the latest encryption standards as defined within FIPS 140-2.	
	SC15	**PUBLICATION 1075 GUIDANCE:** The information system shall prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. Collaborative mechanisms include cameras and microphones that may be attached to the information system. Users must be notified if there are collaborative devices connected to the system.	No collaborative devices are included on or connected to any of the systems that contain FTI.	

	SC17	**PUBLICATION 1075 GUIDANCE:** The agency shall establish PKI policies and practices, as necessary.	PKI is used only for accessing SDT through Tumbleweed and all procedures to establish certificates were followed as required.	
	SC18	**PUBLICATION 1075 GUIDANCE:** 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.	The Tax Department's information systems/computers do not have Internet access and are unable to run mobile code (e.g. Java applets, ActiveX, Flash, etc.).	
	SC19	**PUBLICATION 1075 GUIDANCE:** The agency shall establish, document and control usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies.	The agency currently doesn't use VoIP. If in the future our agency decides to use VoIP; only authorized users will have access to VoIP.	
	SC23	**PUBLICATION 1075 GUIDANCE:** The information system shall provide mechanisms to protect the authenticity of communications sessions.	Communication sessions are protected using transport layer security (TLS). VPN sessions use IPSec.	
8.18	**DATA WAREHOUSE ADDITIONAL COMPUTER SECURITY CONTROLS** Note: These controls are only applicable if the Data Warehouse is implemented in the computer system(s) that store, transmit, or process FTI.			
	DW-	**PUBLICATION 1075**		

	RA	**GUIDANCE:** The agency shall have a Risk Management Program in place to ensure each program is assessed for risk. Risks of the data warehousing environments shall be assessed. Any risk documents shall identify and document all vulnerabilities, associated with the Data Warehousing environment.	The data warehouse is maintained within the Oracle database. Backups occur daily with a weekly back sent off-site. Security controls over the data warehouse is controlled via the RACF security. All components (general mainframe access, audit logs – SMF records, Oracle database, LPAR separations, and MVS operating system) of logical security on the mainframe (with access to the data warehouse) is controlled via the RACF security software. Although the controls are maintained via the mainframe; those controls and the depth of those controls were derived via the Risk Assessment. The Risk Assessment was a formal evaluation of the risks to the FTI, and as such our agency has implemented a set of controls commensurate with those risks identified.	
	DW-PL	**PUBLICATION 1075** **GUIDANCE:** 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	The security plan addresses specific controls related to the data warehouse, and integrates the data warehouse security planning into the agency's overall security procedures. A detailed description of the purpose of the data warehouse, a detailed definition of the database configuration and other unique data warehouse issues.	

		specific details and procedures for security operations. Policies and procedures are required to define how activities and day-to-day procedures will occur. This will contain the specific policies, relevant for all of the security disciplines covered in this document. As this relates to data warehousing, any Data Warehousing documents can be integrated into overall security procedures. A section shall be dedicated to data warehouses to define the controls specific to that environment. Develop policies and procedures to document all existing business processes. Ensure that roles are identified for the organization, regarding the specific roles being created and the responsibilities for these roles. Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing. Define how “legacy system data” will be brought into the data warehouse and how the legacy		

		data that is FTI will be cleansed for the ETL transformation process. The policy shall ensure that FTI will not be subject to Public Disclosure. Only clients or end users can query FTI data with a concrete "need to know".		
	DW-SA	**PUBLICATION 1075 GUIDANCE:** 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.	Prior to the acquisition of any asset, including the components that make up the data warehouse, the security impact is assessed. Specifically for the data warehouse environment the issue of blocking contractor access to the FTI in the database was addressed.	
	DW-CA	**PUBLICATION 1075 GUIDANCE:** Certification, accreditation, and security and risk assessments are accepted best practices used to ensure that appropriate levels of control exist, are being managed and are compliant with all Federal and State laws or statutes. State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in NIST SP 800- 53, February 2005. The process or policy must contain the	The data warehouse environment was included in the most recent risk vulnerability assessment, and data warehouse specific risks are considered as part of the overall system authorization decision by management.	

		methodology being used by the State or local agency to inform management, define accountability and address known security vulnerabilities. Risk assessments should follow the guidelines provided in NIST Publication 800-30 Risk Management Guide for Information Technology Systems, July 2002.		
	DW-PS	**PUBLICATION 1075 GUIDANCE:** 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.	All staff interacting with the data warehouse environment are subject to background screening to ensure suitability for granting access to FTI. Staff that have access to the data warehouse are subject to all agency personnel security controls. See section 8.6 for a detailed description of the personnel security controls.	
	DW-CP	**PUBLICATION 1075 GUIDANCE:**	The data warehouse environment is included in the overall backup and	

		On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. By using new technologies, agencies will ensure the data being provided is reliable. As necessary, based upon risk and cost, these tools shall be implemented. Both incremental and special purpose data back-up procedures are affected, accompanied by off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy, and are tested and verified. Though already addressed in the Publication 1075, this needs to be evaluated to ensure that all data resources are synchronized and restored to allow recreation of the data to take place.	recovery strategy of the Revenue system, which includes backup of the FTI data in the database. See section 8.7 for a detailed description of the contingency planning controls.	
	DW-CM	**PUBLICATION 1075 GUIDANCE:** The agency shall have a process and documentation to identify and analyze how existing FTI is used and how FTI is queried or targeted by end users. FTI parts of the system shall be mapped to follow the flow of the query from a client through the	The data warehouse environment is included in the overall configuration management process for the Revenue system, including the configuration change control board process. See section 8.8 for a detailed description of the configuration management controls.	

		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.		
	DW-MP	**PUBLICATION 1075 GUIDANCE:** 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.	Backup discs are created from the data resident in the data warehouse environment. Those discs are stored in a secure media library on site at the agency's data center. When shipped to the off-site storage vendor the discs are encrypted. Once the disc and FTI residing on it are no longer needed the tape is sanitized by overwriting and destroyed. See section 8.13 for a detailed description of the media protection controls.	
	DW-IR	**PUBLICATION 1075 GUIDANCE:** Intrusion detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data.	The data warehouse environment is included in the overall incident management process for the Revenue system. TIGTA is notified immediately in the event of a compromise of FTI data confidentiality. See section 8.11 for a detailed description of the incident response controls.	
	DW-AT	**PUBLICATION 1075 GUIDANCE:** The agency shall have a "training program" in place that will include	The data warehouse environment is included in the overall security awareness and training process for users and administrators of the	

		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.	Revenue system. See section 8.12 for a detailed description of the security awareness and training controls.	
	DW-IA	**PUBLICATION 1075 GUIDANCE:** The agency shall configure the web services to be authenticated before access is granted to users via an authentication server. Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure only authorized personnel have access to FTI information. Authentication shall be required both at the operating system level and at the application level, when accessing the data warehousing environment.	Unique user identification and authentication is required at the operating system, application and database level within the data warehouse environment. See section 8.14 for a detailed description of the identification and authentication controls.	
	DW-AC	**PUBLICATION 1075 GUIDANCE:** 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	Within the data warehouse environment, FTI is protected as sensitive data and access is restricted to only personnel who need it to fulfill their job responsibility. Access controls are implemented in the database to enforce the restrictions. See section 8.15 for a detailed description of the access controls.	

		shares and directories apply file permissions to ensure only authorized personnel have access to the areas containing FTI. The agency shall have security controls in place that include preventative measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know there is an attack occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations. Within the DW, the agency shall protect FTI as sensitive data and be granted access to FTI for the aspects of their job responsibility. The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job. The agency shall set up access controls in their DW based on personnel clearances. Access controls in a data warehouse are generally classified as 1) General Users; 2) Limited Access Users; and 3) Unlimited Access Users.		

		FTI shall always fall into the Limited Access Users category. All FTI shall have an owner assigned so that there is responsibility and accountability in protecting FTI. Typically, this role will be assigned to a management official such as an accrediting authority. The agency shall configure control files and datasets to enable the data owner to analyze and review both authorized and unauthorized accesses. The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be done at the authentication server. Web-enabled application software shall: 1. Prohibit generic meta-characters from being present in input data 2. Have all database queries constructed with parameterized stored procedures to prevent SQL injection 3. Protect any variable used in		

		scripts to prevent direct OS commands attacks 4. Have all comments removed for any code passed to the browser 5. Not allow users to see any debugging information on the client, and 6. Be checked before production deployment to ensure all sample, test and unused files have been removed from the production system.		
	DW-AU	**PUBLICATION 1075 GUIDANCE:** The agency shall ensure that audit reports are created and reviewed for data warehousing-related access attempts. A data warehouse must capture all changes made to data, including: additions, modifications, or deletions. If a query is submitted, the audit log must identify the actual query being performed, the originator of the query, and relevant time/stamp information. For example, if a query is made to determine the number of people making over $50,000, by John Doe, the audit log would store the fact that John Doe made a query to determine the people who made over $50,000. The results of the query are not as significant as the types of	The data warehouse environment is included in the overall audit and accountability process for the Revenue system. Each level of the data warehouse environment (operating system, database, application) has its own security audit logs that capture security relevant events. See section 8.16 for a detailed description of the auditing controls.	

		query being performed.		
	DW-SC	**PUBLICATION 1075 GUIDANCE:** 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	FTI is encrypted when stored in the data warehouse environment. All sessions of data transfers that contain FTI to and from the data warehouse are encrypted as well using SSL. The data warehouse environment is configured behind the internal firewall for protection. See section 8.17 for a detailed description of the system and communication protection controls.	

		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.		
8.19	**ADDITIONAL COMPUTER SECURITY CONTROLS - TRANSMITTING FTI**			
	ADT1	**PUBLICATION 1075 GUIDANCE:**	Encryption is handled by the Tumbleweed data encryption module.	

		All FTI data in transit must be encrypted, when moving across a Wide Area Network (WAN). Generally, FTI transmitted within the Local Area Network (LAN) should be encrypted. If encryption is not used, the agency must use other compensating mechanisms (e.g., switched vLAN technology, fiber optic medium, etc.) to ensure that FTI is not accessible to unauthorized users.	It meets FIPS 104-2 as indicated by their certificate. FIPS 140-2 standards relate to transmitting encrypted data. When the agency is required by IRS to submit encrypted files, we encrypt the email attachment with 256-bit AES standards.	
	ADT2	**PUBLICATION 1075 GUIDANCE:** 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.	FTI is transmitted via unencrypted fiber optic network. Cables are physically protected in the building by wiring conduits.	

8.20	**ADDITIONAL COMPUTER SECURITY CONTROLS - REMOTE ACCESS**			
	ADR1	**PUBLICATION 1075 GUIDANCE:** Authentication is provided through ID and password encryption for use over public telephone lines.	Remote access occurs via VPN, which is encrypted using the latest encryption standards. If one were to use a public computer (e.g. on a ship or an Internet café); they would have to possess our proprietary VPN software; thus is will not be possible. Further, our Security Policy strictly prohibits the use of public computers for working with FTI.	
	ADR2	**PUBLICATION 1075 GUIDANCE:** Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.	Key Management Centers are maintained on our networks as our agency acts as the certificate Authority using MS Windows features. Backups occur daily with an off-site backup occurring weekly.	
	ADR3	**PUBLICATION 1075 GUIDANCE:** 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	All remote access is through the agency enterprise VPN. There are no toll numbers used for VPN access.	

		as well. Two-factor authentication is recommended whenever FTI is being accessed from an alternate work location.		
8.21	**ADDITIONAL COMPUTER SECURITY CONTROLS - ELECTRONIC MAIL**			
	ADE1	**PUBLICATION 1075 GUIDANCE:** Do not send FTI unencrypted in any email messages. Messages containing FTI must be attached and encrypted. Ensure that all messages sent are to the proper address. Employees should log off the computer when away from the area.	In the rare cases when FTI was sent by email between the Security Manager Tax and the DoT programmer assigned to work with FTI the FTI data was attached and encrypted.	
8.22	**ADDITIONAL COMPUTER SECURITY CONTROLS - FACSIMILE MAIL (FAX)**			
	ADF1	**PUBLICATION 1075 GUIDANCE:** Have a trusted staff member at both the sending and receiving fax machines. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI. Place fax machines in a secured area. Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: A notification of the sensitivity of the data and the need for protection and a notice to	The Division has a policy of not faxing FTI. In the few cases where the Disclosure Office of the IRS has sent a fax to us they first made sure that we were near the fax and ready to receive it.	

		unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.		
9. Agency Disclosure Awareness Program				
9.1	Is there a formal FTI awareness program developed and documented? **Note:** 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 what return information is, and the civil and criminal sanctions for unauthorized inspection or disclosure.	Before any employee of the agency Tax Division or temp worker assigned to the Tax Division begins working in the Division they are required to read and sign a Confidentiality statement which includes Internal Revenue Service Code Sec. 7213 (a) which covers the civil and criminal sanctions. A training in Confidentiality and UNAX is given by the Security Manager of Tax (or his designee) is given at that time. Same training is repeated annually as part of employees' yearly assessment.	