



MIKE DEWINE
★ OHIO ATTORNEY GENERAL ★

Ohio SPR Guidance

Version 1.0

Prepared On: November 28th, 2012

Prepared By: Bradley Picklesimer and Katherine Barga, Internal Audit
Office of Ohio Attorney General
30 East Broad Street 14th floor
Columbus, OH 43215

The purpose of this document is to aid parties, who wish to do business with the Office of the Ohio Attorney General involving records that may contain Federal Tax Information, in completing their required Ohio-SPR (Safeguards Procedure Report) in a complete and accurate manner. The information contained within this document and the FTISP are based on the author(s)'s interpretation of the IRS's Publication 1075 and may not represent the understanding or views of the Office of the Ohio Attorney General (AGO) and/or the IRS. Any factual or material disputes regarding the information contained within are welcome and should be sent directly to the following email address for review and validation: OhioFedTaxInfoSecAudit@OhioAttorneyGeneral.gov. The information contained within this site and program is subject to change; neither the AGO, the IRS nor the author(s)'s of this information are liable for any information contained in this site, nor do they hold any liability for the result(s) of changes to the content. It is the responsibility of the AGO contractor to remain current with the program and to be aware of the laws, regulations, and standards in place governing the Federal Tax Information (FTI) safeguards and in the retention agreement with the AGO.

All of the components for any given control should be responded to. The guidance provided in this document is intended to supplement the control, not replace it. Where a control is not applicable, the agency should clearly indicate why and how it is not applicable. In particular, regarding the technology controls in section 9.0; if for example the controls for public telephone lines are not applicable the agency should indicate that there are no public telephone lines or hardware that would allow the information system to be accessed with them. See each control below for specific additional guidance or email questions to OhioFedTaxInfoSecAudit@OhioAttorneyGeneral.gov.

| Section # | Publication 1075 Requirement <i>Reference pages 38-40, Section 7.2 Safeguard Procedures Report</i> | Ohio-SPR Guidance |
|----------------------------------|---|---|
| 1. Responsible Officer(s) | | |
| 1.1 | Provide the name, title, address, email address and telephone number of the agency official, including but limited to: agency director or named special counsel authorized to request FTI from the OAG. | Provide the complete details requested in the control. IRS Pub 1075: Section 7.2.1 p. 38 |
| 1.2 | Provide the name, title, address, email address and telephone number of the agency official responsible for implementing the safeguard procedures, including but not limited to the agency information technology security office or equivalent and the primary OAG contact. | Internal Audit recommends a secondary person to serve in the absence of the listed official who implements safeguard procedures. IRS Pub 1075: Section 7.2.1 p. 38 |
| 2. Location of the Data | | |
| 2.1 | Provide an organizational chart or narrative description of the receiving agency, which includes all functions within the agency where FTI will be received, processed, stored and/or maintained. If the information is to be used or processed by more than one function, then the pertinent information must be included for each function. Include the number of workers and a description of the position employed to perform each function. Attachments: <i>Organization chart (recommended)</i> | Include how each personnel group or contractor interacts with FTI and the number of employees in each personnel group. Describe how FTI is handled by each group (received, processed, and stored). IRS Pub 1075: Section 7.2.2 p. 38 IRS Pub 1075: Exhibit 12 p. 115 45-day notification to OAG for use of Contractor |
| 3. Flow of the Data | | |
| 3.1 | Provide a flow chart or narrative describing: · the flow of FTI through the agency from its receipt through its return to the AGO or its destruction · how it is used or processed · how it is protected along the way | Describe the flow of FTI through the agency; starting with the request/receipt of records from the OAG through their destruction or return. Describe the flow in terms of the function, including administrative, collections, legal, etc. Describe how the agency uses FTI. Address physical barriers and network security protecting electronic FTI, paper FTI, and the servers within the agency. IRS Pub 1075: Section 7.2.3 p. 39 |
| 3.2 | Describe whether FTI is commingled with agency data or separated. · If FTI is commingled with agency data, please describe how the data is labeled and tracked. · If FTI is separated from all other agency data, please describe the steps that have been taken to keep it in isolation. | If FTI is not commingled, identify as applicable how both electronic and paper FTI are separated from other agency or client data. If the OAG is the agency's only client, identify how FTI is separated from agency's personnel files and other agency specific files. If FTI is commingled, describe how it is labeled and tracked; both electronically and in paper format. Also, |

| | | |
|-----|---|--|
| | | <p>describe what compensating measures are in place to secure all records if they cannot be separated.</p> <p>IRS Pub 1075: Section 7.2.3 p. 39</p> |
| 3.3 | <p>Provide a list of the FTI extracts the agency receives and whether the data is received through electronic or non-electronic methods.</p> | <p>Response is already provided by OAG:</p> <p>Agency receives the following FTI extracts on assigned accounts, all through electronic methods via FTP:</p> <p><u>The TOPs Refund Information</u> containing the amount of federal refund withheld and the “TOPS” designator.</p> <p><u>PIT100 Certification Files</u> received from Taxation and assigned to agency for collection. Certain personal income tax (“PIT”) accounts transmitted through electronic means from Collections Enforcement to Agency contain FTI extracts. The types of PIT account and the corresponding FTI contained therein are detailed below.</p> <ul style="list-style-type: none"> - Source Code 13 (delinquency assessment): Taxpayer’s name, mailing address, SSN, the source code, tax year and Ohio tax amount due - Source Code 18 (FAGI audit assessment): the source code, tax year and the Ohio tax amount due - Source Code 21 (IRS Revenue Agent Report assessment): the source code, tax year and the Ohio tax amount due - Source Code 29 (CP 2000 assessment): the source code, tax year and the Ohio tax amount due |
| 3.4 | <p>Describe the paper or electronic products created from FTI (e.g. letters, agency reports, data transcribed, spreadsheets, electronic database query results). Only include those products created by your agency (i.e. do not include reports provided to your agency by Collections Enforcement).</p> | <p>Include dunning letters, legal filings, spreadsheets, back-ups, etc. Any paper or electronic item created from the information contained in an OAG debt record with the Source Code(s) listed in 3.3 should be treated as potential FTI.</p> |
| 3.5 | <p>Describe where contractors are involved in the flow of FTI including, but not limited to, data processing, disposal, analysis, modeling, maintenance, etc.</p> | <p>Include any contractors working less than the two minimum barriers of security required to FTI; consider IT contractors, software maintenance, skip tracing, shred, building owners/maintenance etc. Describe how each contractor is involved with FTI, or would have access to FTI or the information system.</p> <p>IRS Pub 1075: Section 7.4.5 p. 41</p> |
| 3.6 | <p>Describe the following for each contractor:</p> <ul style="list-style-type: none"> · Name of each Contractor · Contractor Work Location (Address) · Support contractor provides for the agency · Identify the FTI the contractor has access to (data files, data elements, systems, applications) · State whether or not contractor's employees have completed required disclosure awareness training and signed confidentiality agreements. If not, explain. | <p>Complete the template provided for each contractor listed in 3.5 and any other section of the SPR, where the contractor is less than two minimum barriers of security to FTI. All contracts must include Exhibit 7 language, and addition to agency imposed confidentiality or other agreements. If not included, provide a date of completion.</p> <p>IRS Pub 1075: Section 7.4.5 p. 41 IRS Pub 1072: Exhibit 7 p. 98</p> |

| | | |
|--------------------------------------|---|--|
| | <ul style="list-style-type: none"> · State whether or not the legal contract between the agency and the contractor includes the Publication 1075, Exhibit 7 language. If not, explain. · State whether or not any FTI is provided to contractors or contractor information systems off-shore. If yes, explain. · If IT support is provided by a state run data center, state whether or not there an SLA in place between the agency and the data center operations. If not, explain. <p>* Please note that the AGO generally does not permit special counsel and third party vendors to employ subcontractors where the contract requires the redisclosure of FTI.</p> | |
| 4. System of Records | | |
| 4.1 | <p>Describe the permanent record(s) (logs) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes or cartridges or other removable media) (e.g. FTI receipt logs, transmission logs, or destruction logs in electronic or paper format.) Please include a sample of the agency logs.</p> <p>Attachments: <i>Sample agency logs (recommended)</i></p> | <p>Your agency is responsible to maintain a log and to document requests for, receipt of, distribution of and disposition of FTI independent of any other agency. A system of record keeping should be developed, maintained, and retained for audit.</p> <p>Provide a sample of agency log.</p> <p>IRS Pub 1075: Section 7.2.4 p. 39</p> |
| 5. Secure Storage of the Data | | |
| 5.1 | <p>Describe how the agency meets minimum protection standards (including compliance with two barriers between FTI and someone unauthorized to access FTI). Include a description of how the agency controls physical access to FTI, controls access to computer facilities, offsite storage, and interior work environments.</p> | <p>Include physical barriers to office and any rooms where FTI is stored, i.e. locked doors, badge access, security guards, locked filing cabinets, etc. Include systemic barriers to electronic FTI, i.e. multiple passwords, need to know access, etc.</p> <p>Include barriers for any location FTI may be accessed including home office, offsite storage, alternate work sites, etc.</p> <p>Offsite storage should include any place tape or other backups are stored.</p> <p>Alternate work site are any location the agency would use to access OAG records other than the primary location(s) provided in other parts of this document.</p> <p>IRS Pub 1075: Section 4.2 p. 20, p. 28</p> |
| 5.2 | <p>Describe the policies and procedures in place for protecting the facilities or rooms containing or accessing FTI.</p> <ul style="list-style-type: none"> · Describe how the agency maintains key records (e.g. key issuance, how many keys are available) · Describe how the agency regularly conducts periodic reconciliation on all key records | <p>Indicate and maintain a log for who has access devices (key, badge, fob, combination, etc.) to locked barrier to FTI. How many access devices are available, by type? Include the frequency of reconciliation period on access devices. Where are blank and unused access devices stored? What measures are in place to secure the system(s) used to activate access devices? Are all changes of access logged?</p> <p>IRS Pub 1075: Section 4.3.10 p. 24</p> |

| | | |
|---|--|--|
| <p>5.3</p> | <p>Describe the policies and procedures in place for meeting minimum protection standards for alternative work sites (e.g. employee’s homes or other non-traditional work sites).</p> | <p>If alternative work sites are not used, describe policies and systemic protections preventing access to the agency’s information systems and FTI.</p> <p>If alternative work sites are used, how are minimum protection standards enforced? What are the procedures in place regarding remote access? Address policies and systemic protections against unauthorized use of remote access.</p> <p>IRS Pub 1075: Section 4.7 p. 26</p> |
| <p>6. Restricting Access to the Data</p> | | |
| <p>6.1</p> | <p>Describe the procedures taken to ensure that access to FTI is restricted to those that have a “need to know”. This includes a description of:</p> <ul style="list-style-type: none"> · How the information will be protected from unauthorized access when in use by the authorized recipient · Systemic or procedural barriers | <p>Describe how both electronic and paper FTI are protected from those that do not have a “need to know”, i.e. passwords, locks, locking computers when away from desk, clean desk policy, etc. Address the restriction of FTI when unauthorized contractors or personnel are in areas with FTI.</p> <p>IRS Pub 1075: Section 5.2 p.29 IRS Pub 1075 Exhibit 8 p. 104</p> |
| <p>6.2</p> | <p>Describe any existing agreements created under the authority of IRC 6103 (p) (2) (B), if applicable. Identify the agency to whom your agency is providing the data to and the type of data received.</p> | <p>No agency has been granted the right to re-disclose FTI accounts under the authority of IRC 6103 (p)(2)(B) or other governing statute. Should a need for re-disclosure arise a written agreement with the OAG would have to be obtained and approved prior to any re-disclosure of FTI.</p> <p><i>No response required.</i></p> |
| <p>7. Other Safeguards</p> | | |
| <p>7.1</p> | <p>Describe the agency’s process for conducting internal inspections of headquarters, field offices, data center, offsite storage, and contractor sites.</p> <p>Attachments: <i>Internal Inspections Plan (recommended)</i></p> | <p>What is the agency’s process and frequency of internal inspections? Address how incidents/deficiencies discovered during inspections will be handled. Include inspections of all areas where FTI is received, stored, processed, or destroyed. Include a copy of the agency internal inspections plan.</p> <p>IRS Pub 1075: Section 6.3 p.35</p> |
| <p>7.2</p> | <p>Describe the process for detecting and monitoring deficiencies identified during audits and internal inspections and how they are tracked in a Plan of Actions and Milestones (POA&M).</p> | <p>Describe how deficiencies are detected and monitored during audits and internal inspections. Use a POA&M to track what you find and fix during internal inspections and as a basis for your annual SAR (Safeguard Activity Report).</p> <p>IRS Pub 1075: Section 6.4 p.37</p> |
| <p>8. Disposal</p> | | |
| <p>8.1</p> | <p>Describe the method(s) of FTI disposal (when not returned to the AGO) and a sample of the destruction log. For example, burning and shredding are acceptable methods of FTI disposal. Identify the specifications for each destruction method used (e.g. shred size).</p> <p>If FTI is returned to the AGO, provide a description of the procedures.</p> <p>Attachments: <i>Destruction Log Template (recommended)</i></p> | <p>How are paper and electronic (screen prints, reports, case files, removable/portable media, hard drives, etc.) FTI disposed. Include disposal specifications for each method used, including shred size. Provide a destruction log template that includes records destroyed, date/time of destruction, and the agency official responsible for the destruction.</p> <p>IRS Pub 1075: Section 8.3 p.44</p> |
| <p>9. Information Technology (IT) Security</p> | | |

| | | |
|-------|--|---|
| 9.1.1 | Provide the name and address where the agency's IT equipment resides (e.g. data center, computer room). | Provide the full address, even if it is the same as an address provided previously in this or another document. |
| 9.1.2 | Describe the following pertaining to data center or computer room operations: <ul style="list-style-type: none"> Identify if the facility is operated by a consolidated state-wide data center, a private contractor, or entirely by the agency Describe other state agencies and/or departments that have access to this facility Describe whether FTI access is granted to other agencies or tribes | Address the building, room, cage, rack, and system level(s) of access unauthorized personnel, IT contractors, or other vendors have to the agency information system(s) containing FTI. |
| 9.1.3 | Provide the name, title, address, telephone number, and e-mail address of the IT Security Administrator or other IT contact responsible for administering the equipment. | Provide the full details requested in the control even if this person is listed elsewhere in the document. Internal Audit recommends a secondary person to serve in the absence of the listed official who is responsible for administering the equipment. |
| 9.1.4 | Provide a brief description of the electronic flow of FTI within all IT equipment and network devices that process, receive, store, transmit and/or maintain the data. | Include how FTI is received electronically and then moves through the agency's information systems. Include the flow across a network map; switches, routers, servers, and end users interface with the data. |
| 9.1.5 | Provide an inventory of all IT equipment and network devices that process, receive, store, transmit and/or maintain the data (e.g. routers, switches, firewalls, servers, mainframes, and workstations). For each device, identify the following: <ul style="list-style-type: none"> Platform (e.g. Mainframe, Windows, Unix/Linux, Router, Switch, Firewall) <ul style="list-style-type: none"> If mainframe, number of production LPARs with FTI, security software (e.g. RACF, ACF2) If not mainframe, number of production servers or workstations that store or access FTI. Operating System (e.g. zOS v1.7, Windows 2008, Solaris 10, IOS) Application Software (Commercial Off The Shelf or custom) used to access FTI <ul style="list-style-type: none"> Software used to retrieve FTI (e.g. SDT (Tumbleweed), CyberFusion, Connect:Direct) | Include platform (desktop, laptop, tablet, etc.), operating system, application software used to access FTI, software used to retrieve FTI. Include number and type of client computers; indicate which if any have remote access. Include server(s), operating system, and network appliance that comprise the information system. |
| 9.2 | Management Security Controls: Risk Assessment Control Family | |
| 9.2.1 | Describe how the agency develops, documents, disseminates, and updates, as necessary, risk assessment policy and procedures to facilitate implementing risk assessment controls. Such risk assessment controls include risk assessments and risk assessment updates. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.14 p.54 NIST Vulnerability Database: RA-1 |

| | | |
|-------|---|--|
| 9.2.2 | Describe how agencies 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. Describe how the agency updates 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. | Describe how the agency conducts assessments of the risk and magnitude of harm that could result from the unauthorized activities in a holistic level. Describe how the agency updates the risk assessment periodically or whenever there are significant changes IRS Pub 1075: Section 9.14 p.54 NIST Vulnerability Database: RA-3 |
| 9.2.3 | Describe how the agency scans systems containing FTI, at a minimum, quarterly to identify vulnerabilities in the information system. Describe how the agency's vulnerability scanning tool(s) must be updated with the most current definitions prior to conducting a vulnerability scan. | Include how the scanning tool will be operated, reports generated, the review process of the reports, including frequency of review, and remediation efforts if a deficiency is found. Address frequency of scans and the updating of scanning tools. If vulnerability scans are not being used, indicate when they will be in place. IRS Pub 1075: Section 9.14 p.54 NIST Vulnerability Database: RA-5 |
| 9.3 | Management Security Controls: Security Planning Control Family | |
| 9.3.1 | Describe how the agency develops, documents, disseminates, and updates, as necessary, security planning policy and procedures to facilitate implementing security planning controls. Such security planning controls include system security plans, system security plan updates and rules of behavior. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.13 p.54 NIST Vulnerability Database: PL-1 |
| 9.3.2 | Describe how the agency develops, documents, and establishes a system security plan (see Publication 1075 Section 7.2, Safeguard Procedures Report) by describing the security requirements, current controls and planned controls, for protecting agency information systems and federal tax information (FTI). Describe how the agency's system security plan is updated to account for significant changes (see Publication 1075 Section 7.4, Annual Safeguard Activity Report) in the security requirements, current controls and planned controls for protecting agency information systems and FTI. | Elaborate on how the plan is maintained and at a high level describe the system security plan, i.e. the security requirements, current and planned controls, for protecting FTI. If agency does not have plan in place, indicate the expected date of plan completion. IRS Pub 1075: Section 9.13 p.54 NIST Vulnerability Database: PL-2 |
| 9.3.3 | Describe how the agency develops, documents, and establishes a set of rules identifying their responsibilities and expected behavior for information system use for users of the information system. | How are rules (acceptable use of technology and records, etc.) developed, documented and established. Include how updates and/or training are implemented. If agency does not conduct such assessments, indicate the expected date of plan completion. IRS Pub 1075: Section 9.13 p.54 NIST Vulnerability Database: PL-4 |
| 9.3.4 | For Federal agencies, describe how the agency conducts a privacy impact assessment on the information system in accordance with | <i>No response required. However if the agency does perform PIA, respond to the control.</i> |

| | | |
|-------|---|---|
| | OMB policy. Note: <i>This control is only required for Federal agencies.</i> | |
| 9.3.5 | Describe how the agency plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. | What considerations are made to minimize the impact of security related events? Consider upgrades, new systems, responding to alarm/monitoring failure, or an actual event. IRS Pub 1075: Section 9.13 p.54 NIST Vulnerability Database: PL-6 |
| 9.4 | Management Security Controls: System and Services Acquisition Control Family | |
| 9.4.1 | Describe how the agency develops, documents, disseminates, and updates, as necessary, system and services acquisition policy and procedures to facilitate implementing system and services acquisition controls. Such system and services acquisition controls include information system documentation and outsourced information system services. Describe how the agency ensures that there is sufficient information system documentation, such as a Security Features Guide. Also, describe how the agency ensures third-party providers of information systems, who are used to process, store and transmit FTI, employ security controls consistent with Safeguard computer security requirements. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.15 p.54 NIST Vulnerability Database: SA-1 |
| 9.4.2 | Describe how the agency documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system. | How is the budget allocated for information system protection resources? IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-2 |
| 9.4.3 | Describe how the agency manages the information system using a system development life cycle methodology that includes information security considerations, whenever information systems contain FTI. | Describe software and hardware upgrades and updates, methodology, and analysis used. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-3 |
| 9.4.4 | Describe how the agency includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk, whenever information systems contain FTI. Ensure the description acknowledges that the contract for the acquisition must contain IRS Publication 1075 Exhibit 7 language as appropriate. | Describe how agency assesses risk and considers its security needs when making IT purchases and completing network setups. System acquisition contracts should be completed, with Exhibit 7 language, if further relationship exists between agency and IT system providers. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-4 IRS Pub 1072: Exhibit 7 p. 98 |
| 9.4.5 | Describe how the agency obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information systems, whenever information systems contain FTI. | Address how agency obtains and protects information system documentation such as systems and software documentation, network diagrams, proprietary source code, or other intellectual property that may lead to compromising the systems. Indicate any authorization controls to view FTI documents. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-5 |

| | | |
|--------|---|---|
| 9.4.6 | Describe how the agency complies with software usage restrictions, whenever information systems contain FTI. | Address how compliance with software usage restrictions are achieved. Consider use of unlicensed software, End User License Agreements (EULA), acceptable use policies, etc. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-6 |
| 9.4.7 | Describe how the agency enforces explicit rules governing the installation of software by users, whenever information systems contain FTI. | Indicate if user has the ability to install software. Elaborate on controls preventing the installation of software by unauthorized personnel. Address the process used to determine what software can be installed on a device that may contain or have access to FTI. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-7 |
| 9.4.8 | Describe how the agency designs and implements the information system using security engineering principles, whenever information systems contain FTI. | What guidelines does agency use to implement IT security engineering principles, i.e. guidelines for security objectives, secure design guidelines, patterns, principles, threat models, architecture and design reviews for security, performing regular code reviews for security, testing for security, and conducting deployment reviews to ensure secure configuration, etc. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-8 |
| 9.4.9 | Describe how the agency performs configuration management during information system design, development, implementation, and operation; and manages and controls changes to the information system. Describe how the agency implements only agency-approved changes, documents approved changes to the information system(s) and tracks security flaws and flaw resolution. | Include how configuration management is performed during information system design, development, implementation, and operation. Discuss the management and controlling of changes and using only agency-approved changes. Describe how security flaws and flaw resolution are tracked. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-9 |
| 9.4.10 | Describe how agency information system developers create a security test and evaluation (ST&E) plan, implement the plan, and document the results. | Create a ST&E plan for all changes made in the production environment. Consider risk and vulnerabilities in a holistic manner, i.e. internal threats, viruses, malware, regression testing, etc. Include all testing completed and the documenting of results. IRS Pub 1075: Section 9.15 p.55 NIST Vulnerability Database: SA-10 |
| 9.5 | Management Security Controls: Security Assessment and Authorization Control Family | |
| 9.5.1 | Describe how the agency develops and updates a policy that addresses the processes used to test, validate, and authorize the security controls used to protect FTI. While state and local agencies are not required to conduct a NIST compliant certification & accreditation (C&A), the agency shall accredit in writing that the security controls have been adequately implemented to protect FTI. Describe how the agency institutes a written accreditation process, constituting the agency's acceptance of the security controls and associated risks. | At this time, agency need only describe the process used to develop and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. Include the testing, validation and authorization of security controls used to protect FTI. Address the written accreditation process. IRS Pub 1075: Section 9.5 p.49 NIST Vulnerability Database: CA-1 |

| | | |
|-------|---|--|
| 9.5.2 | Describe how the agency conducts, periodically but at least annually, an assessment of the security controls in the information system to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This assessment shall complement the certification process to ensure that periodically the controls are validated as being operational. The assessment must be documented in writing. | Document the process of the annual conduction of security control assessments. Pair off the assessments from the accreditation process from 9.5.1 to ensure controls are adequate to secure FTI. IRS Pub 1075: Section 9.5 p.49 NIST Vulnerability Database: CA-2 |
| 9.5.3 | Describe how the agency authorizes and documents 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. Describe how the agency conducts 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. | How are connections to other information systems authorized and documented, i.e. network diagrams displaying connections and interfaces. Elaborate how agency ensures controls are operating as intended. A system of monitoring should be in place that will only allow secure systems to connect remotely, a remote system health monitor, etc. Keep in mind the connection to the AGO and other business partners. IRS Pub 1075: Section 9.5 p.50 NIST Vulnerability Database: CA-3 |
| 9.5.4 | Describe how the agency develops and updates a Plan of Action & Milestones (POA&M) that identifies any deficiencies related to FTI processing. Describe how the POA&M identifies planned, implemented, and evaluated remedial actions to correct deficiencies noted during internal inspections. Also, ensure to address the Corrective Actions Plan (CAP) that identifies activities planned or completed to correct deficiencies identified during the on-site safeguard review. Both the POA&M and the CAP shall address implementation of security controls to reduce or eliminate known vulnerabilities in the system. | Create a POA&M to identify and document any deficiencies related to FTI processing. POA&M is intended to track internal discovery of deficiencies and remediation through the entire time you are working with the OAG. Further, this will serve as a basis for agency's annually required Safeguard Activity Report (SAR). IRS Pub 1075: Section 9.5 p.50 NIST Vulnerability Database: CA-5 |
| 9.5.5 | Describe how owners of FTI accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the security authorization. All information regarding the authorization shall be provided to the Office of Safeguards as part of the Safeguard Activity Report. | Address the validation of protections for FTI prior to operation and the plan to reauthorize security controls with regard to changes in the control structure. Address the frequency of accreditation process and approval of security authorization. IRS Pub 1075: Section 9.5 p.50 NIST Vulnerability Database: CA-6 |
| 9.5.6 | Describe how the agency periodically, at least annually, monitors the security controls within the information system hosting FTI to ensure that the controls are operating, as intended. | Address security monitoring particulars, its frequency, and how agency validates they are working properly. IRS Pub 1075: Section 9.5 p.50 NIST Vulnerability Database: CA-7 |

| 9.6 | Operational Security Controls: Personnel Security Control Family | |
|-------|--|---|
| 9.6.1 | Describe how the agency develops, documents, disseminates, and updates as necessary, personnel security policy and procedures to facilitate implementing personnel security controls. Such personnel security controls include position categorization, personnel screening, personnel termination, personnel transfer, and access agreements. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-1 |
| 9.6.2 | Describe how the agency assigns risk designations to all positions and establish screening criteria for individuals filling those positions. | Indicate risk assigned to each position (collector, attorney, IT support, administrative, etc.) handling FTI. Different groups with different levels of access and monitoring will pose varying levels of risk. Describe the screening criteria for each position, i.e. background checks, credit checks, employment history validation, validation of applicant identity, etc. IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-2 |
| 9.6.3 | Describe how individuals are screened before authorizing access to information systems and information. | Include interviews, background checks, credits checks, employment history validation, validation of applicant identity, etc. Is required training, and contract work validated etc. IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-3 |
| 9.6.4 | Describe how the agency terminates information system access, conduct exit interviews, and ensures return of all information system-related property when employment is terminated. | Discuss terminating information system access, exit interviews, and ensuring the return of all information system-related property such as laptops and cellphones. How long does system access termination take? IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-4 |
| 9.6.5 | Describe how the agency reviews information system access authorizations and initiates appropriate actions when personnel are reassigned or transferred to other positions within the agency. | Include how information system access is authorized and initiated. Address the periodic review of information system access. IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-5 |
| 9.6.6 | Describe how appropriate access agreements are completed before authorizing access to users requiring access to the information system and FTI. | Include agreements with the required language for access to FTI. IRS Pub 1075: Section 9.12 p.53 NIST Vulnerability Database: PS-6 |
| 9.6.7 | Describe how personnel security requirements are established for third-party providers and monitored for provider compliance. | Include non-disclosure agreements, confidentiality agreements, the use of Exhibit 7 language, background checks, etc. Third parties who may have access to FTI should be held to the same standards prescribed for your staff. IRS Pub 1075: Section 9.12 p.53 IRS Pub 1072: Exhibit 7 p. 98 NIST Vulnerability Database: PS-7 |
| 9.6.8 | Describe how the agency establishes a formal sanctions process for personnel who fail to comply with established information security policies, as this relates to FTI. | What are the sanctions in place regarding infractions relating to FTI? Understanding that consistent implementation of the sanctions is an audit criterion. |

| | | |
|--------------|---|--|
| | | IRS Pub 1075: Section 9.12 p.54 IRS Pub 1075: Exhibit 5 p.95 NIST Vulnerability Database: PS-8 |
| 9.7 | Operational Security Controls: Contingency Planning Control Family | |
| 9.7.1 | <p>Describe how the agency develops applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches.</p> <p>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.</p> | <p>At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion.</p> <p>IRS Pub 1075: Section 9.7 p.51 NIST Vulnerability Database: CP-1 and CP-2</p> |
| 9.7.2 | <p>For Federal agencies, describe how personnel are trained in their contingency roles and responsibilities with respect to the information system and provide refresher training at least annually.</p> <p><i>Note: This control is only required for Federal agencies.</i></p> | <p><i>No response required. However if the agency is training personnel with contingency roles provide a response to the control.</i></p> |
| 9.7.3 | <p>Describe how the agency periodically tests contingency plans 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.</p> | <p>Describe contingency plan testing, the frequency of the testing, and how FTI is safeguarded during testing.</p> <p>IRS Pub 1075: Section 9.7 p.51 NIST Vulnerability Database: CP-4</p> |
| 9.7.4 | <p>Describe how the agency identifies alternate storage sites and initiates necessary agreements to permit the secure storage of information system and FTI backups.</p> | <p>Does the agency have alternate storage sites? If so, what agreements are in place? Has the agency performed a risk assessment on the facilities?</p> <p>IRS Pub 1075: Section 9.7 p.51 NIST Vulnerability Database: CP-6</p> |
| 9.7.5 | <p>Describe how the agency identifies alternate processing sites and/or telecommunications capabilities, and initiates 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.</p> | <p>Does the agency have alternate processing sites? If so, what agreements are in place? Has the agency performed a risk assessment on the facilities?</p> <p>IRS Pub 1075: Section 9.7 p.51 NIST Vulnerability Database: CP-7</p> |
| 9.8 | Operational Security Controls: Configuration Management Control Family | |
| 9.8.1 | <p>Describe how the agency develops, documents, disseminates, and updates as needed, configuration management policy and procedures to facilitate implementing configuration management security controls.</p> | <p>At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion.</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-1</p> |

| | | |
|--------------|--|---|
| <p>9.8.2</p> | <p>Describe how the agency develops, documents, and maintains a current baseline configuration of the information system.</p> | <p>Baseline configuration management creates a history of configuration changes when managing hardware, software, firmware, documentation, etc. The initial baseline is current state, which ideally is functional, secure, and stable. Then changes to the baseline should be documented as technology is upgraded, maintenance, etc. Periods of significant change may warrant a significant state to be documented, or a realignment of the baseline. This history will help identify when and where deficiencies occur, in addition to providing considerations for future states when exploring new technologies or upgrades.</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-2</p> |
| <p>9.8.3</p> | <p>Describe how the agency authorizes, documents, and controls changes to the information system.</p> | <p>Who authorizes changes to the information system? How are changes controlled? Are change requests documented, validated, tested, etc.</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-3</p> |
| <p>9.8.4</p> | <p>Describe how the agency analyzes changes to the information system to determine potential security impacts prior to change implementation.</p> | <p>Include testing and analysis of changes to the information system. Does testing contain data received from the OAG?</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-4</p> |
| <p>9.8.5</p> | <p>Describe how the agency approves 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.</p> | <p>Who approves access privileges? Address the generating, retaining, and reviewing of records.</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-5</p> |
| <p>9.8.6</p> | <p>Describe how the agency establishes mandatory configuration settings for information technology products employed within the information system, which (i) configures the security settings of information technology products to the most restrictive mode consistent with operational requirement; (ii) documents the configuration settings; and (iii) enforces the configuration settings in all components of the information system.</p> <p><i>Note: IRS Office of Safeguards requires mandatory system configuration settings identified in Computer Security Evaluation Matrices (SCSEM). These tools are available on IRS.gov, keyword "Safeguards Program".</i></p> | <p>How is access limited to staff members, address the documentation of the configuration systems, how does the agency enforce the configuration systems?</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-6</p> |
| <p>9.8.7</p> | <p>Describe how the agency implements the following least functionality requirements:</p> <ul style="list-style-type: none"> · Describe how the agency restricts access for change, configuration settings, and provides the least functionality necessary. · Describe how the agency enforces access restrictions associated with changes to the information system. · Describe how the agency configures the security settings of information technology products to the most restrictive mode | <p>Least functionality is the principle for providing users the absolute minimum amount of access or ability, while still allowing them to perform the tasks required. Regarding the five points of the control, demonstrate how the agency keeps the minimum number of people with only the access they require to perform their task(s).</p> <p>IRS Pub 1075: Section 9.6 p.50 NIST Vulnerability Database: CM-7</p> |

| | | |
|-------|---|--|
| | <p>consistent with information system operational requirements. (For additional guidance see NIST SP 800-70 Security Configuration Checklists Program for IT Products- Guidance for Checklists Users and Developers)</p> <ul style="list-style-type: none"> · Describe how the agency configures the information system to provide only essential capabilities. · Describe how the agency identifies and prohibits the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting FTI. | |
| 9.8.8 | Describe how the agency develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. | <p>Maintain an inventory list of information system equipment in use by each employee, network appliances, servers, etc. Include a reconciliation period for inventory.</p> <p>IRS Pub 1075: Section 9.6 p.51 NIST Vulnerability Database: CM-8</p> |
| 9.9 | Operational Security Controls: Maintenance Control Family | |
| 9.9.1 | Describe how the agency develops, documents, disseminates, and updates, as necessary, maintenance policy and procedures to facilitate implementing maintenance security controls. Such maintenance security controls include identifying and monitoring a list of maintenance tools and remote maintenance tools. | <p>At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion.</p> <p>IRS Pub 1075: Section 9.10 p.52 NIST Vulnerability Database: MA-1</p> |
| 9.9.2 | Describe how the agency ensures that maintenance is scheduled, performed, and documented. Describe how the agency reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. | <p>Include the frequency of maintenance and how it is performed and documented. Include the review of maintenance records.</p> <p>IRS Pub 1075: Section 9.10 p.53 NIST Vulnerability Database: MA-2</p> |
| 9.9.3 | Describe how the agency approves, controls, and routinely monitors the use of information system maintenance tools and remotely-executed maintenance and diagnostic activities. | <p>Include the approval method and the monitoring and controlling of maintenance tools.</p> <p>IRS Pub 1075: Section 9.10 p.53 NIST Vulnerability Database: MA-3 and MA-4</p> |
| 9.9.4 | Describe how the agency allows only authorized personnel to perform maintenance on the information system. | <p>Is there a validation of maintenance between IT and the management or is maintenance at the sole discretion of IT? Address controls preventing unauthorized personnel from performing maintenance; consider this down to the workstation level.</p> <p>IRS Pub 1075: Section 9.10 p.53 NIST Vulnerability Database: MA-5</p> |
| 9.10 | Operational Security Controls: System and Information Integrity Control Family | |

| | | |
|--------|--|--|
| 9.10.1 | Describe how the agency develops, documents, disseminates and updates, as necessary, system and information integrity policy and procedures to facilitate implementing system and information integrity security controls. Such system and information integrity security controls include flaw remediation, information system monitoring, information input restrictions, and information output handling and retention. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.17 p.56 NIST Vulnerability Database: SI-1 |
| 9.10.2 | Describe how the agency identifies, reports, and corrects information system flaws. | How are flaws identified, who are flaws reported to, describe the correction of flaws. Include testing, validation, and implementation processes in flaw mediation. IRS Pub 1075: Section 9.17 p.57 NIST Vulnerability Database: SI-2 |
| 9.10.3 | Describe how the agency's information systems implement protection against malicious code (e.g., viruses, worms, Trojan horses) that, to the extent possible, includes a capability for automatic updates. | Do scans occur on a real-time basis, scheduled basis, or both? Who has the ability to circumvent the malicious code protection mechanisms? Are there detection techniques in place to alert abnormalities in the environment? How are detection systems updated and patched? IRS Pub 1075: Section 9.17 p.56 NIST Vulnerability Database: SI-3 |
| 9.10.4 | Describe how the agency's intrusion detection tools and techniques are employed to monitor system events, detect attacks, and identify unauthorized use of the information system and FTI. | Identify the software used. How is detection method configured to identify unauthorized use of FTI? IRS Pub 1075: Section 9.17 p.56 NIST Vulnerability Database: SI-4 |
| 9.10.5 | Describe how the agency receives and reviews information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response. | How are alerts received, reviewed, issued to appropriate personnel, and appropriate actions taken? Is there an expected SLA and are events tiered for severity? IRS Pub 1075: Section 9.17 p.57 NIST Vulnerability Database: SI-5 |
| 9.10.6 | Describe how the agency restricts information system input to authorized personnel (or processes acting on behalf of such personnel) responsible for receiving, processing, storing, or transmitting FTI. | Describe restrictions in place preventing unauthorized access to FTI. Are passwords unique to each user? IRS Pub 1075: Section 9.17 p.57 IRS Pub 1075 Exhibit 8 p. 104 NIST Vulnerability Database: SI-9 |
| 9.10.7 | Describe how the agency handles and retains output from the information system, as necessary to document that specific actions have been taken. | Plan for a minimum of 6 years of retention for FTI output. IRS Pub 1075: Section 9.17 p.57 NIST Vulnerability Database: SI-12 |
| 9.11 | Operational Security Controls: Incident Response Control Family | |

| | | |
|------------------------|---|--|
| <p>9.11.1</p> | <p>Describe how the agency develops, documents, disseminates, and updates as necessary incident response policy and procedures to facilitate the implementing incident response security controls. These policies and procedures must cover both physical and information system security relative to the protection of FTI. Such incident response security controls include incident response training and incident reporting and monitoring.</p> | <p>At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion.</p> <p>IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-1</p> |
| <p>9.11.2</p> | <p>Describe how the agency trains personnel with access to FTI, including contractors and consolidated data center employees if applicable, in their incident response roles on the information system and FTI. Incident response training must provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication, and recovery.</p> | <p>Describe incident response training to include preparation, detection and analysis, containment, eradication, and recovery. Address how incidents are handled, who is notified, etc.</p> <p>IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-2</p> |
| <p>9.11.3</p> | <p>Describe how the agency tests and/or exercises the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results.</p> | <p>Develop a test plan that is exercised at least annually. The plan should include how an incident is responded to, what parties will be involved in resolving the incident, appropriate reporting, resolving issues from the fall out of the breach, and a review for lessons learned to update policy(s) and security to prevent future incident(s).</p> <p>IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-3</p> |
| <p>9.11.4</p> | <p>Describe how the agency routinely tracks and documents all physical and information system security incidents potentially affecting the confidentiality of FTI.</p> | <p>How are physical and systemic unauthorized access attempts tracked and documented?</p> <p>IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-5</p> |
| <p>9.11.5</p> | <p>Describe the agency's policy to immediately report incident information any time there is a compromise to FTI to the appropriate Agent-in-Charge and the OAG's designee. The OAG will handle communications with TIGTA and the IRS.</p> | <p>Include the reporting to OAG's Disclosure Officer. What information would the agency provide to the OAG post incident? Agent-in-Charge is whomever the agency designates to work with the OAG, IRS, TIGTA, and there designees in the event of an incident.</p> <p>IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-6</p> |
| <p>9.11.5.1</p> | <p>Describe the agency's policy on communication of an incident; including how employees and contractors have been trained to handle media or public inquiries regarding an incident. Incident communication procedures should be part of annual compliance training.</p> | <p>Include that the agency will turn all media or public inquiries to the OAG.</p> <p>IRS Pub 1075: Section 9.9 p.52</p> |

| | | |
|--------|---|--|
| 9.11.6 | Describe how the agency provides an incident response support resource (e.g. help desk) that offers advice and assistance to users of the FTI and any information system containing FTI for the handling and reporting of security incidents. Describe how the support resource is an integral part of the agency's incident response capability. | Appoint an employee or implement an incident response support source. Include how the support resource is an integral part of the agency's incident response capability. IRS Pub 1075: Section 9.9 p.52 NIST Vulnerability Database: IR-7 |
| 9.12 | Operational Security Controls: Security Awareness and Training Control Family | |
| 9.12.1 | Describe how the agency develops, documents, disseminates, and updates as necessary, awareness and training policy and procedures to facilitate implementing awareness and training security controls. Such awareness and training security controls include security awareness and security training. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.4 p.49 NIST Vulnerability Database: AT-1 |
| 9.12.2 | Describe how the agency ensures all information system users and managers are knowledgeable of security awareness material before authorizing access to the system. | How is personnel trained on security awareness material? Include additional training on a periodic basis or when updates are implemented. IRS Pub 1075: Section 9.4 p.49 NIST Vulnerability Database: AT-2 |
| 9.12.3 | Describe how the agency identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides sufficient security training before authorizing access to the information system and FTI. | Identify personnel with significant security roles and responsibilities (functional managers, IT personnel, etc.). Address additional training and the documentation that corresponds to these personnel. IRS Pub 1075: Section 9.4 p.49 NIST Vulnerability Database: AT-3 |
| 9.12.4 | Describe how the agency documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. | Include the frequency of training review, how is it documented, who monitors training? Address at a high level the content of security training activities. IRS Pub 1075: Section 9.4 p.49 NIST Vulnerability Database: AT-4 |
| 9.13 | Operational Security Controls: Media Access Protection Control Family | |
| 9.13.1 | Describe how the agency develops, documents, disseminates, and updates as necessary, media access policy and procedures to facilitate implementing media protection policy. Policies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-1 |
| 9.13.2 | Describe how the agency restricts access to information system media to authorized individuals, where this media contains FTI. | If agency does not allow removable media, describe the systemic or policy preventions of using removable media. Consider tape, CD/DVD, flash memory, external hard drives, etc. as portable/removable media. If agency has removable media, how is it secured from those unauthorized to access it. IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-2 |

| | | |
|--------|--|---|
| 9.13.3 | Describe how the agency labels removable media (CDs, magnetic tapes, external hard drives, flash/thumb drives, DVDs) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "FTI". Notice 129-A and Notice 129-B can be used for this purpose. | If agency has removable media, detail how it is labeled indicating "FTI". IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-3 |
| 9.13.4 | Describe how the agency physically controls and securely stores information system media within controlled areas, where this media contains FTI. | How are removable media, back-up drives, paper FTI, etc. controlled and securely stored from unauthorized access? IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-4 |
| 9.13.5 | Describe how the agency protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Describe the agency's use of transmittals or equivalent tracking method to ensure FTI reaches its intended destination. | If media is not transported outside of the office, indicate as such. If media is transported outside of office, how is it protected and controlled en route. Include logging at final destination, employees that travel with media, the destruction of media, etc. An inventory of the media should exist where it is created, used, stored, and destroyed; demonstrating the complete lifespan of the media. Inventory should be reconciled regularly. IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-5 |
| 9.13.6 | Describe how the agency sanitizes information system media prior to disposal or release for reuse. | Include the methods and details surrounding electronic media destruction. IRS Pub 1075: Section 9.11 p.53 NIST Vulnerability Database: MP-6 |
| 9.14 | Technical Security Controls: Identification and Authentication Control Family | |
| 9.14.1 | Describe how the agency develops, documents, disseminates, and updates, as necessary, identification and authentication policy and procedures to facilitate implementing identification and authentication security controls. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.8 p.51 NIST Vulnerability Database: IA-1 |
| 9.14.2 | Describe how the agency's information system(s) must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validates users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics. | If used, describe password standards; how often personnel are required to change the password, password complexity, etc. Two factor authentications are optimal. IRS Pub 1075: Section 9.8 p.52 IRS Pub 1075 Exhibit 8 p. 104 NIST Vulnerability Database: IA-2 and IA-3 |

| | | |
|----------------------|--|---|
| <p>9.14.3</p> | <p>Describe how the agency manages user accounts assigned to the information system. Examples of effective user-account management practices include (i) obtaining authorization from appropriate officials to issue user accounts to intended individuals; (ii) disabling user accounts timely; (iii) archiving inactive or terminated user accounts; and (iv) developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by the information system.</p> | <p>Include all points of control: obtaining authorization to issue accounts, timely disabling of accounts, archiving inactive or terminated accounts, validating users who request reinstatement. Include who has the authority to assign and restrict user access and the process used to coordinate changing user account access.</p> <p>IRS Pub 1075: Section 9.8 p.52 NIST Vulnerability Database: IA-4</p> |
| <p>9.14.4</p> | <p>Describe how the agency’s information system(s) obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.</p> | <p>How is the password obscured when keyed into the system? When the error message displays indicating login failure, is any information provided that could lead to exploitation?</p> <p>IRS Pub 1075: Section 9.8 p.52 IRS Pub 1075 Exhibit 8 p. 104 NIST Vulnerability Database: IA-6</p> |
| <p>9.14.5</p> | <p>Whenever agencies are employing cryptographic modules, describe how the agency works to ensure these modules are compliant with NIST guidance, including FIPS 140-2 compliance.</p> | <p>If cryptographic modules are used, address at a high level how modules are FIPS 140-2 compliant.</p> <p>IRS Pub 1075: Section 9.8 p.52 FIPS Pub 140-2 NIST Vulnerability Database: IA-7</p> |
| <p>9.15</p> | <p>Technical Security Controls: Access Control Family</p> | |
| <p>9.15.1</p> | <p>Describe how the agency develops, documents, disseminates, and updates, as necessary, access control policy and procedures 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.</p> | <p>At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion.</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-1</p> |
| <p>9.15.2</p> | <p>Describe how the agency manages information system user accounts, including establishing, activating, changing, reviewing, disabling, and removing user accounts.</p> | <p>Include who is responsible for assigning and restricting profiles, what constitutes the establishment, activating, changing, etc. of user accounts.</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-2</p> |
| <p>9.15.3</p> | <p>Describe how the agency’s information system(s) enforce assigned authorizations for controlling system access and the flow of information within the system and between interconnected systems.</p> | <p>Agency should address access control policies and access enforcement mechanisms employed by the agency between users and the information system.</p> <p>Access control policy (identity, role, attribute based policy, etc.), is the documented method by which the agency intends to control access. Access enforcement (access control list, access control matrices, cryptography, etc.), is any method(s) used to enforce the access policy and prevent unauthorized users from accessing FTI, and limited authorized users to only what they need.</p> |

| | | |
|--------|--|--|
| | | <p>Information system (computers, servers, media, files, records, processes, domains, network equipment, etc.), is any equipment that compromise the information system containing FTI.</p> <p>Where interconnected systems are present, those used for FTI and those used for any other purpose, the agency will need to address how these two controls are implemented to regulate access to the FTI from a connected system. How does the agency regulate both user access to and the flow of information between these types of systems?</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-3 and AC-4</p> |
| 9.15.4 | Describe how the agency ensures that only authorized employees or contractors (if allowed by statute) of the agency receiving the information has access to FTI. For example, human services agencies may not have access to FTI provided to child support enforcement agencies or state revenue agencies. | <p>Include how access capability controls are enforced. Address separation of duties regarding access to FTI, i.e. how is the IT consultant systemically separated from FTI?</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-5</p> |
| 9.15.5 | Describe how agency information system(s) enforce the most restrictive access capabilities users need (or processes acting on behalf of users) to perform specified tasks. | <p>Do employees have limited access controlled by their work functions? How is this control implemented?</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-6</p> |
| 9.15.6 | Describe how agency information system(s) 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. | <p>Include the number of consecutive unsuccessful attempts, the timeframe of these attempts, how the limit is enforced, and the start-up requirements after an account is locked.</p> <p>IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-7</p> |
| 9.15.7 | <p>Describe how the agency’s information system(s) display an approved system usage notification or warning banner before granting system access informing potential users that</p> <ul style="list-style-type: none"> (i) The system contains U.S. Government information (ii) Users actions are monitored and audited (iii) Unauthorized use of the system is prohibited (iv) Unauthorized use of the system is subject to criminal and civil sanctions. The warning banner must be applied at the application, database, operating system and network device level for all system types that receive, store, process and transmit FTI. (See Publication 1075, Exhibit 13 for example warning banners). <p>Describe how the policy is 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.</p> <p>Attachments: <i>Sample warning banner in use (required)</i></p> | <p>Provide a sample warning banner that includes all points of control. If banner is not in place, provide an estimated date of implementation. At what point of inactivity will the banner be displayed? Banner is required at all points of entry to the information system containing FTI.</p> <p>IRS Pub 1075: Section 9.2 p.47 IRS Pub 1075: Exhibit 5 p.95 IRS Pub 1075: Exhibit 13 p. 117 NIST Vulnerability Database: AC-8</p> |

| | | |
|---------|--|--|
| 9.15.8 | Describe how the agency identifies and documents specific user actions that can be performed on the information system without identification or authentication. | Can user perform any functions on the information system without identification or authentication? If so, describe those functions. IRS Pub 1075: Section 9.2 p.47 NIST Vulnerability Database: AC-14 |
| 9.15.9 | Describe how the agency authorizes, documents, and monitors all remote access capabilities used on the system, where these systems containing FTI. | Discuss the authorization, documenting, and monitoring of all remote access capabilities. Address systemic or procedural barriers in place preventing unauthorized personnel from remote access. IRS Pub 1075: Section 9.2 p.48 NIST Vulnerability Database: AC-17 |
| 9.15.10 | Describe how the agency develops 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. | Address systemic procedures in place preventing wireless access capabilities to FTI systems. If used, develop a policy including the authorization, documentation, and monitoring of all wireless access. Policy should also be included if remote access users could be using wireless externally. IRS Pub 1075: Section 9.2 p.48 NIST Vulnerability Database: AC-18 |
| 9.15.11 | Describe how the agency develops policies for any allowed portable and mobile devices, where these systems contain FTI. As part of this, the agency shall authorize, document, and monitor all device access to organizational information systems accessing FTI. | Address if the use of portable devices is prohibited systematically with a DLP or MDM solution. If not, develop a policy including the authorization, documentation, and monitoring or all device access. IRS Pub 1075: Section 9.2 p.48 NIST Vulnerability Database: AC-19 |
| 9.15.12 | Describe how the agency develops policies for authorized individuals to access the information systems from an external system, such as access allowed from an alternate work site. Describe how the agency's policy addresses the authorizations allowed to receive, transmit, store, and/or process FTI. As part of this, describe how the agency authorizes, documents, and monitors all access to organizational information systems, where these systems contain FTI. | Include the authorization, documentation, and monitoring of remote access. Address the minimum protection standards surrounding remote access. If not used, address policies and controls in place preventing remote access. IRS Pub 1075: Section 9.2 p.48 NIST Vulnerability Database: AC-20 |
| 9.16 | Technical Security Controls: Audit and Accountability Control Family | |
| 9.16.1 | Describe how the agency develops, documents, disseminates, and updates as necessary, audit and accountability policy and procedures to facilitate implementing audit and accountability security controls. Such audit and accountability security controls include auditable events; content of audit records; audit storage capacity; audit processing; audit review, analysis and reporting; time stamps; protecting audit information and audit retention. | At this time, agency need only describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.3 p.48 IRS Pub 1075: Exhibit 9 p. 106 NIST Vulnerability Database: AU-1 |

| | | |
|--------|--|--|
| 9.16.2 | Describe how the agency's information system(s) 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. | Discuss the process used to generate and review audit records. At a high level, address the content of the audit logs. Audit records should include logins to the system, logins to FTI processing applications, changes of access or rights, actions taken with FTI while processing records, any failures, etc. IRS Pub 1075: Section 9.3 p.48 NIST Vulnerability Database: AU-2 |
| 9.16.3 | Describe how the agency's identified security-relevant events enable the detection of unauthorized access to FTI data. System and/or security administrator processes will include all authentication processes to access the system, for both operating system and application-level events. Describe how audit logs enable tracking of activities to take place on the system. | Address controls that detect internal and external attempts to access FTI by an unauthorized person. Also, consider detection of virus, malware, network abnormalities, breach and other security related events. IRS Pub 1075: Section 9.3 p.48 NIST Vulnerability Database: AU-3 |
| 9.16.4 | Describe how the agency configures the information system to allocate sufficient audit record storage capacity to record all necessary auditable items. | How is storage allocated to stored audit records for a 6 year retention period? IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-4 |
| 9.16.5 | Describe how the agency's information system(s) alert appropriate organizational officials in the event of an audit processing failure and take additional actions. | Who is alerted in the event of audit failures? Describe the procedures in place regarding a failure and the additional actions after notification. IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-5 |
| 9.16.6 | Describe how the agency routinely reviews audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution. | Indicate the personnel and frequency of audit record review. Who are findings reported to and describe any corrective action taken. IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-6 |
| 9.16.7 | Describe how the agency's information system(s) provide an audit reduction and report generation capability to enable review of audit records. | Indicate if audits can be filtered or configured to omit mundane and routine information and to consolidate the audit logs into actionable intelligence. IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-7 |
| 9.16.8 | Describe how the agency's information system(s) provide date and time stamps for use in audit record generation. | Are date and time stamps provided on all audit records? How does the information system date/time stamp events? IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-8 |
| 9.16.9 | Describe how the agency's information system(s) protect audit information and audit tools from unauthorized access, modification, and deletion. | In responding to this control, the agency should have a base line of settings for the audit capabilities of its information system. This allows for testing to ensure the audit system(s) are fully functional, and can easily be restored if needed. Audit logs should write to a secure location on the information system and be read-only. Access to the audit logs and system(s) that generate them should be limited to an absolute minimum. These logs and systems should require special permissions to delete, and at minimum by policy be protected from deletion for any audit record less than six years of retention. IRS Pub 1075: Section 9.3 p.49 |

| | | |
|----------------|---|---|
| | | NIST Vulnerability Database: AU-9 |
| 9.16.10 | Describe how the agency ensures that audit information is archived for <u>six years</u> to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored. | Address the six year retention period and the secure requirement for retention of audit information. IRS Pub 1075: Section 9.3 p.49 NIST Vulnerability Database: AU-11 |
| 9.17 | Technical Security Controls: System and Communications Protection Control Family | |
| 9.17.1 | Describe how the agency develops, documents, disseminates and updates as necessary, system and communications policy and procedures to facilitate implementing effective system and communications. | At this time, the agency needs only to describe the process used to develop, document disseminate, and update policy. The policy itself will be requested at a future date. If agency does not have policy in place, indicate the expected date of policy completion. IRS Pub 1075: Section 9.16 p.55 NIST Vulnerability Database: SC-1 |
| 9.17.2 | Describe how the agency's information system(s) separate front end interfaces from the back end processing and data storage. | Address systemic barriers preventing the end user from accessing the database information directly. IRS Pub 1075: Section 9.16 p.55 NIST Vulnerability Database: SC-2 |
| 9.17.3 | Describe how the agency's information system(s) prevent unauthorized and unintended information transfer via shared system resources. | Consider email and the Internet as shared system resources, in addition to share drives, cloud space, or other common resources. How is information transfer prevented via shared system resources? IRS Pub 1075: Section 9.16 p.55 NIST Vulnerability Database: SC-4 |
| 9.17.4 | Describe how the agency's information system(s) are configured to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. | How are controls configured to monitor the boundaries? If data is moving from the segment of your information system that is authorized for FTI how does the agency know? What is implemented to prevent this type of exfiltration? IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-7 |
| 9.17.5 | Describe how the agency's information system(s) protect the confidentiality of FTI during electronic transmission. | How is FTI protected, i.e. encryption, secure channels, etc.? Address controls that prevent additional transmission of FTI that is not protected. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-9 |
| 9.17.6 | Whenever there is a network connection, describe how the agency's information system(s) terminate network connections at the end of a session or after no more than fifteen minutes of inactivity. | Indicate the timeframe in which network connections are terminated after period of inactivity. How are these controls implemented? IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-10 |
| 9.17.7 | Whenever Public Key Infrastructure (PKI) is used, describe how the agency establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. | How does agency establish and manage cryptographic keys? If PKI is not used by agency, indicate as such. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-12 |

| | | |
|---------|--|---|
| 9.17.8 | Whenever cryptography (encryption) is employed, describe how the agency's information system(s) 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. | If cryptography is not used by agency, indicate as such. If used, address how agency's cryptography meets the FIPS 140-2 standard. IRS Pub 1075: Section 9.16 p.56 IRS Pub 1075: Exhibit 10 p. 108 FIPS Pub 140-2 NIST Vulnerability Database: SC-13 |
| 9.17.9 | Describe how the agency's information system(s) prohibit remote activation of collaborative computing mechanisms without 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. | Indicate if the agency has collaborative devices (microphones, web cams, etc.) in its environment. Address systemic barriers preventing the remote activation of collaborative mechanisms. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-15 |
| 9.17.10 | Whenever Public Key Infrastructure (PKI) is used, describe how the agency establishes PKI policies and practices. | If PKI is not used, indicate as such. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-17 |
| 9.17.11 | Describe how the agency establishes 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. | Address policies and controls that prevent the use of mobile code. Address personal devices brought to the agency that can access Wi-Fi or remote connection. Mobile code should address items such as Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-18 |
| 9.17.12 | Describe how the agency establishes, documents, and controls usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies. | If VoIP is not used, indicate as such. If VoIP is used, how is it established, documented and usage restriction controlled? IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-19 |
| 9.17.13 | Describe how the agency's information system(s) provide mechanisms to protect the authenticity of communications sessions. | Address the method used to secure the channel and protect its authenticity. Sessions are defined as any connection to or from the information system containing FTI where data transfer, access, modification is possible. Consider when the agency is connected to the OAG to receive records, etc. IRS Pub 1075: Section 9.16 p.56 NIST Vulnerability Database: SC-23 |
| 9.17.14 | For Federal agencies, describe how information system components reside in separate physical domains (or environments) as deemed necessary. Note: This control is only required for Federal agencies. | <i>No response required. However, if the agency has this type of separate physical environments, describe.</i> |
| 9.18 | Additional Information Technology Controls – Data Warehouse Environment | |

| | | |
|----------------------|--|---|
| <p>9.18.1</p> | <p>Describe how the agency implements a risk management program to ensure each aspect of the data warehouse is assessed for risk. Describe how the agency’s risk documents identify and document all vulnerabilities, associated with the data-warehousing environment.</p> | <p>Unless the agency has a data warehouse as defined below, the controls in section 9.18 can be omitted by indicating, “Data warehousing is not in use at our agency”.</p> <p>A data warehouse <i>is</i> a historical collection of records that are not modified, but are used for research and to generate reports based on the historical information. Trend analysis of the data to drive business decisions constitute the practice of data warehousing. This same practice with active records, is real time data warehousing may require your organization to respond to section 9.18</p> <p>If your agency can be identified as practicing any of the functions mentioned above you should readdress the controls in section 9.18 as they relate to the data warehousing activities and hardware in use at your agency.</p> <p>IRS Pub 1075: Section 9.18.1 p.57 IRS Pub 1075: Exhibit 11 p. 109</p> |
| <p>9.18.2</p> | <p>Planning is crucial to the development of a new environment. Describe the agency’s implementation of a security plan to address organizational policies, security testing, rules of behavior, contingency plans, architecture/network diagrams, and requirements for security reviews. While the plan will provide planning guidelines, this will not replace requirements documents, which contain specific details and procedures for security operations.</p> <p>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.</p> <p>Describe how the agency implements policies and procedures to document all existing business processes. The agency must ensure that roles are identified for the organization and develop responsibilities for the roles.</p> <p>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.</p> <p>The agency must define how “legacy system data” will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the ETL transformation process.</p> | <p>Response is not applicable if agency does not have a data warehouse as defined in 9.18.1.</p> |

| | | |
|---------------|---|---|
| | The policy shall ensure that FTI will not be subject to public disclosure. Only authorized users with a demonstrated “need to know” can query FTI data within the data warehouse. | |
| 9.18.3 | Acquisition security needs to be explored. As FTI is used within data warehousing environments, describe how services and acquisitions have adequate security in place, including blocking information to contractors, where these contractors are not authorized to access FTI. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.4 | <p>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.</p> <p>Describe how the agency implements a process or policy to ensure that data warehousing security meets the baseline security requirements defined in the current revision of NIST SP 800-53. The process or policy must contain the methodology being used by the state or local agency to inform management, define accountability and address known security vulnerabilities.</p> <p>Risk assessments must follow the guidelines provided in NIST Publication 800-30 Risk Management Guide for Information Technology Systems.</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.5 | Describe personnel security controls for the data warehouse environment. 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. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.6 | There are no additional physical security controls for a data warehousing environment. However, describe the physical security requirements throughout Publication 1075 which do apply to the physical space hosting the data warehouse hardware. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.7 | On line data resources shall be provided adequate tools for the back-up, storage, restoration, and validation of data. Agencies will ensure the data being provided is reliable. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |

| | | |
|----------------|--|---|
| | <p>Both incremental and special purpose data back-up procedures are required, combined with off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy, and are tested and verified.</p> <p>Describe the content of the agency's contingency plan. Ensure that the data warehouse is addressed to allow for restoration/recreation of data to take place.</p> | |
| 9.18.8 | <p>During the life cycle of the DW, on-line and architectural adjustments and changes will occur. Describe the process for managing these DW configuration changes. Ensure that the agency documents these changes and assures that FTI is always secured from unauthorized access or disclosure.</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.9 | <p>Describe the policy and procedures in place for the cleansing process at the staging area and how the ETL process cleanses 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 to be removed by a random overwrite software program.</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.10 | <p>Describe the agency's policy and procedures for incident response as it pertains to the data warehousing environment.</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.11 | <p>Describe the agency's disclosure awareness training program. Ensure that training addresses 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.</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.12 | <p>The agency shall configure the web services to be authenticated before access is granted to users via an authentication server. The web portal and 2-factor authentication requirements in Publication 1075 Section 9 apply in a data warehouse environment.</p> <p>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.</p> <p>Describe the identification and authentication policy and procedures as they pertain to the data warehousing environment. Authentication shall be required both at the operating system level and at the application level, when accessing the data warehousing</p> | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |

| | | |
|---------|--|---|
| | environment. | |
| 9.18.13 | <p>Describe which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure only authorized personnel have access to the areas containing FTI.</p> <p>Describe the 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.</p> <p>Within the DW, describe how the agency protects FTI and grants access to FTI as it relates to aspects of a user’s job responsibility. Describe how the agency enforces effective access controls so that end users have access to programs with the least privilege needed to complete the job. Describe how the agency configures 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.</p> <p>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.</p> <p>Web-enabled application software shall:</p> <ol style="list-style-type: none"> 1. Prohibit generic meta-characters from being present in input data 2. Have all database queries constructed with parameterized stored procedures to prevent SQL injection 3. Protect any variable used in scripts to prevent direct OS commands attacks 4. Have all comments removed for any code passed to the browser 5. Not allow users to see any debugging information on the client 6. Be checked before production deployment to ensure all sample, test and unused files have been removed from the production system | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.18.14 | Describe the agency’s audit and accountability policy and procedures as it pertains to creating and reviewing audit reports for data-warehousing-related access attempts. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |

| | | |
|--------|--|---|
| 9.18.5 | <p>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. Describe how the agency segregates the data warehouse's production and test environments.</p> <p>Describe how the agency ensures the following:</p> <ul style="list-style-type: none"> · All Internet transmissions should be encrypted using HTTPS protocol utilizing Secure Sockets Layer (SSL) encryption based on a certificate containing a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This will allow information to be protected between the server and the workstation. During the Extract, Transform and Load stages of data entering a warehouse, data is at its highest risk. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption, i.e., from workstation to point of data. · Web server(s) that receive online transactions shall be configured in a "Demilitarized Zone" (DMZ) in order to receive external transmissions but still have some measure of protection against unauthorized intrusion. · Application server(s) and database server(s) shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers. · Transaction data shall be "swept" from the web server(s) at frequent intervals consistent with good system performance, and removed to a secured server behind the firewalls, to minimize the risk that these transactions could be destroyed or altered by intrusion. · Anti-virus software shall be installed and maintained with current updates on all servers and clients that contain tax data. · For critical online resources, redundant systems shall be employed with automatic failover capability. | Response is not applicable if agency does not have a data warehouse as defined in 9.18.1. |
| 9.19 | Additional Information Technology Controls – Transmitting FTI | |
| 9.19.1 | <p>Describe the policy and procedures in place that address how the agency secures FTI data while in transit. All FTI data in transit must be encrypted, when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN).</p> <p>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.</p> | <p>What methods are used to secure FTI data in transit, i.e. encryption? Identify policies or controls in place preventing unsecured FTI from being transmitted. All agencies with access to FTI for any purpose transmit the data to some level.</p> <p>IRS Pub 1075: Section 9.18.2 p.57 IRS Pub 1075: Exhibit 10 p. 108</p> |
| 9.19.2 | <p>Indicate whether or not unsecured cable circuits are used by the agency. If in use, describe measures being taken to secure unencrypted cable circuits.</p> | <p>Identify if cable circuits or FTI is encrypted. How are cable circuits physically protected?</p> <p>IRS Pub 1075: Section 9.18.2 p.57</p> |

| | | |
|---------------|---|--|
| | <p>Unencrypted cable circuits of copper or fiber optics is an acceptable means of transmitting FTI. Measures must be taken to ensure that circuits are maintained on cable and not converted to unencrypted radio (microwave) transmission. Additional precautions must 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).</p> <p>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.</p> | |
| 9.20 | Additional Information Technology Controls – Remote Access | |
| 9.20.1 | <p>Describe how the agency secures communications over public telephone lines. Authentication should be provided through ID and password encryption for use over public telephone lines.</p> | <p>Is FTI transmitted over public telephone lines? If so, is authentication provided through ID and password encryption? If not, identify policies or systemic controls preventing transmission of FTI over public telephone lines. If this control is not applicable because the agency does not have public telephone lines and/or the equipment needed to hook them to the information system and provide access; state that.</p> <p>IRS Pub 1075: Section 9.18.3 p.57 IRS Pub 1075: Exhibit 10 p. 108</p> |
| 9.20.2 | <p>Describe how the agency controls and enforces key management. Authentication is controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.</p> | <p>Control refers to electronic keys used for cryptographic purposes. Indicate if key management is utilized by agency. If used, how is key management enforced and controlled?</p> <p>IRS Pub 1075: Section 9.18.3 p.57</p> |
| 9.20.3 | <p>Describe the agency’s remote telephone access procedures.</p> <p>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 must have both identification and authentication features and must provide data encryption as well. Two-factor authentication is required whenever FTI is being accessed from an alternate work location or if accessing FTI via the agency’s web portal.</p> | <p>If not used, identify any policies or controls in place preventing remote access. If used, include two-factor authentication and access method details.</p> <p>IRS Pub 1075: Section 9.18.3 p.57 IRS Pub 1075: Exhibit 10 p. 108</p> |
| 9.21 | Additional Information Technology Controls – Internet | |
| 9.21.1 | <p>Describe the agency’s policy and procedures for restricting access to sensitive data on systems that connect to the Internet. Describe the types of security measures employed.</p> | <p>Include the restriction of access to sensitive data while system is connected to the internet. How would the agency be aware of a system connect to the Internet that was breached?</p> <p>If application is used to restrict access and filtering, provide a description of application. Include what information is set to be considered sensitive and how it handles data exfiltration, intentional or otherwise.</p> <p>IRS Pub 1075: Section 9.18.4 p.58</p> |

| | | |
|---------------|--|--|
| 9.22 | Additional Information Technology Controls – Electronic Mail (E-mail) | |
| 9.22.1 | <p>Describe the agency’s policy and procedures toward transmitting FTI via E-mail. If E-mail is used to transmit FTI, describe the secure measures implemented to safeguard FTI.</p> <p>If transmittal of FTI within the agency’s internal e-mail system is necessary, the following precautions must be taken to protect FTI sent via E-mail:</p> <ul style="list-style-type: none"> · Do not send FTI unencrypted in any email messages · The file containing FTI must be attached and encrypted · Ensure that all messages sent are to the proper address · Employees must log off the computer when away from the area. | <p>If not used, include how FTI is systemically prevented from being emailed. If not systematically prevented, a policy must be developed regarding all points of control.</p> <p>If FTI is transmitted via E-mail include response to all points of control.</p> <p>IRS Pub 1075: Section 9.18.5 p.58</p> |
| 9.23 | Additional Information Technology Controls – Facsimile Mail (FAX) | |
| 9.23.1 | <p>Describe the agency’s policy and procedures for transmitting FTI via FAX.</p> <p>Securing FAX transmissions will include:</p> <ul style="list-style-type: none"> · Having a trusted staff member at both the sending and receiving fax machines. · Maintaining broadcast lists and other preset numbers of frequent recipients of FTI. · Placing fax machines in a secured area. · Including a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: A notification of the sensitivity of the data and the need for protection and a notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information. | <p>If not used, include how FTI is systemically prevented from being faxed. If not systematically prevented, a policy must be developed regarding all points of control.</p> <p>If FTI is transmitted via fax, include response to all points of control. Include that agency should instruct on the fax, unauthorized disclosure should request the recipient to call them back to ensure proper destruction of the records and logging of the incident.</p> <p>IRS PUB 1075: SECTION 9.18.6 P.58</p> |
| 9.24 | Additional Information Technology Controls – Multi-Functional Printer-Copier Devices | |
| 9.24.1 | <p>Describe the agency’s policy and procedures for transmitting FTI via multi-functional printer-copier devices.</p> <p>If the agency uses a multi-functional printer-copier device, specific requirements regarding FTI must be followed.</p> <ul style="list-style-type: none"> · FTI must be encrypted in transit either to or from the device. · FTI must not be emailed or faxed from the device. · If FTI is scanned into the device, the user must authenticate on the device with a unique username and password. · FTI may not be stored locally on the device | <p>If not used, include how FTI is systemically prevented from being transmitted via multi-functional printer-copier devices. If not systematically prevented, a policy must be developed regarding all points of control.</p> <p>If FTI is transmitted via multi-functional printer-copier devices, include response to all points of control.</p> <p>IRS Pub 1075: Section 9.18.7 p.58</p> |
| 9.25 | Additional Information Technology Controls – Live Data Testing | |
| 9.25.1 | <p>Describe the agency’s policy and procedures for testing with live FTI data.</p> | <p>Indicate if agency currently tests with live FTI data. If used, describe all policies, procedures, the testing environments, tests conducted, etc. that include live FTI data.</p> <p>IRS Pub 1075: Section 9.18.8 p.59</p> |

| | | |
|----------------------|---|--|
| <p>9.26</p> | <p>Additional Information Technology Controls – Web Portal</p> | |
| <p>9.26.1</p> | <p>Describe the agency’s policy and procedures for use of web portals when providing FTI over the Internet to customers.</p> <p>To utilize a web portal that provides FTI over the Internet to a customer, the agency must meet the following requirements:</p> <ul style="list-style-type: none"> · The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI and access to the database through the application is limited. · Each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the web portal is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing. · Access to FTI via the web portal requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication. | <p>Indicate if agency currently uses web-portals for providing information to customers, or indicate the control is not applicable as this service is not provided.</p> <p>IRS Pub 1075: Section 9.18.9 p.59</p> |
| <p>9.27</p> | <p>Additional Information Technology Controls – Integrated Voice Response (IVR) Systems</p> | |
| <p>9.27.1</p> | <p>Describe the agency’s policy and procedures for IVR system usage.</p> <p>To utilize an IVR system that provides FTI over the telephone to a customer, the agency must meet the following requirements:</p> <ul style="list-style-type: none"> · The LAN segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system. · The operating system and associated software for each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing. · Independent security testing must be conducted on the IVR system prior to implementation. · Access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties | <p>Indicate if agency uses an IVR system, and respond accordingly if IVR is in use.</p> <p>IRS Pub 1075: Section 9.18.10 p.59</p> |

| | | |
|---|---|--|
| | involved and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication. | |
| 9.28 | Additional Information Technology Controls – Emerging Technologies | |
| 9.28.1 | Describe the agency’s policy and procedures for maintaining FTI safeguards standards when using emerging technologies. Emerging technologies are those not explicitly mentioned in this document and authorization is to be granted by the OAG no less than 45-days prior to implementing said technology. | If the agency has any technology in use that was not implicitly addressed in this document, while receiving, storing, processing, or disposing of FTI it should be noted here. Agency should also define what safeguards are in place to protect FTI while this technology is in use. (It is recommended the agency fully address controls, such as the minimum protection standards etc. for each technology in an attachment.) IRS Pub 1075: Section 9.18.11 p.60 |
| 10. Disclosure Awareness Program | | |
| 10.1 | Describe the agency’s formal disclosure awareness program. Provide procedure information for initial and annual certification. Provide a sample copy of training materials presented to employees and contractors. Attachments: <i>Documentation of each employee’s signed initial certification/annual recertification of disclosure awareness training and sample copy of training materials (required)</i> | Provide each employee’s signed initial certification or annual recertification of disclosure awareness training. Provide a sample copy of training materials. IRS Pub 1075: Exhibit 5 p.95 IRS Pub 1075: Exhibit 6 p.97 |