

**Safeguard Symposium & Security Officers Conference  
Previously Submitted Questions**

**Could you please provide details as to the logistics of creating and maintaining logs to satisfy the record keeping requirements of IRS Publication 1075?**

- Recognizing some of the overall requirements, such as the need to know, audit trails and accountability, should electronic logs be individually maintained and accounted for by each employee that receives and has custody of federal tax information (fti)?
- Or, would it suffice to locate the log in a shared electronic file that can be updated by several employees and perhaps viewed by many more? If this approach is sufficient, please note that accountability and audit trails for changes to the log would be lost since multiple people could change the log contents. The file would only indicate the employee who made the last changes. It would also allow multiple people to view fti being utilized by other employees.

**Along the same lines as the above question, and in an effort to reduce the forwarding of paper fti and its recording in logs:**

- Can paper audit files with commingled fti be scanned into electronic files to provide both short and long term storage solutions and to lessen the log-keeping burden?
- To facilitate this, multiple Departmental personnel would require read access to the documents at certain times during the appeals period. Could this be accomplished through giving access to groups of personnel within the applicable divisions, or should these rights be granted only on an as needed basis, such as when an appeal has been made?
- Would this do away with the logging requirements necessary for paper documents?

**Are electronic signatures sufficient for employee acknowledgment of awareness training?**

**Is FTI encryption a requirement when moving across a WAN even when the network utilizes VPN technologies?**

- If so, should the FTI be included in an attachment & compliant with FIPS 140-2?

What about the encryption requirements within a closed Departmental e-mail system?

- Specifically, should the forwarding of any TDS acknowledgment or other FTI information be encrypted in an attachment and compliant with FIPS 140-2?

**Could you expand on the assignment of risk designations to all positions and the screening criteria for individuals filling those positions?**

- Does this screening include agency transfers?
- Would a background check satisfy the screening requirement?

**Are there tools or resources available to assist and document the annual certification and accreditation process?**

- Who should conduct them?

**Is two-factor authentication simply a recommendation or is it a requirement for accessing FTI from alternate work locations?**

**Mobile Devices (Laptops, smart phones) and Wireless Access**

Sections 4.7 Alternate Work Sites and 5.6.17.3 Remote Access, define safeguards for remote access sites, but do not address laptops, smart phones, or other portable media devices used by traveling staff. These staff may be accessing the information via a laptop (or other mobile devices) at locations other than a home office or remote office site using a wireless connection (Wifi, or cell modem) using a secured encrypted communication product (in this case CITRIX) . An example may be a Child Protection and Safety worker addressing an emergency investigation and placement at the child's home.

- 1) What safeguards are required to address mobile media and wireless access to accommodate this type of business requirement?
- 2) What documentation is the state agency required to provide during their security review?

**Risk Assessment section 5.6.13**

Who is responsible for performing the risk assessment. Is that something that we should do on our own, contract out through our Office of the CIO, or have a third party come in and perform the assessment? What are the guidelines from the IRS?

**Identification and Authentication section 5.6.7**

I'm assuming that this section pertains only to systems that contain or access FTI. In regards to cryptography, it appears that it is optional at this time?

**What are the guidelines for FTI data at rest on a hard drive. Will it need to be encrypted?**

**When transferring data from a workstation to the mainframe, will the data need to be encrypted prior to being sent via an SSL connection or can the transfer be the only thing encrypted?**

**What are the guidelines for disaster recovery of FTI?** If we have FTI stored properly on a standalone machine . . . . and there is something catastrophic that happens to the building. What are the guidelines for making a backup copy of this information?

**We would like physical security touched on. Do we need to have enclosed, locked rooms for users that access FTI?**

**Does IRS have an audit plan or questionnaire for conducting internal inspections?**

IRS requires Internal Inspection be performed by the recipient agency. The purpose is to ensure those adequate safeguards are security measures have been maintained. Copies of the internal inspection should be submitted to IRS with the annual Safeguard activity Report. Reviews are conducted within an 18-month cycle. The inspection should be conducted by a function other than the using function.

**What does the IRS expect the states to do to secure the data from the IRS once it is received from SDT?** I have reviewed the PUB 1075 and the Safeguards Technical Assistance Memorandum. There is a statement that the data must be encrypted while at rest on the server. What do you consider at rest? Also what are the retention periods of the files? How long should we keep the files encrypted on the state servers? I understand that there should be an automated process to keep the files cleaned up. Also what are the requirements if the data received from SDT is loaded into a database on the state server for processing what are the requirements there?

**Could you address the proper procedure for obtaining an expert witness from the IRS on our criminal cases?** It used to be that we would request this through the Disclosure Office and then the players changed and they would not respond to our request. We then issued a subpoena for the expert witness and we were told that they did not have to respond to the subpoena. We would just like to have clarification on the proper procedure. We were referred to the regulation 11.3.35.10 for a statement regarding the need for the witness, however, at the end of this section, it also talks about the agency being able to waive this requirement.

**What is the exact wording on the warning banners?** What was provided in the recommendation on the report and what was faxed to me by the reviewer was different. It would be beneficial if all the states had the same wording.

**Do you have examples of what they send out to the states prior to the review?**

**Do you have CD/DVD of a UNAX movie to show to contractors?**

**Remote worksite guidance?** Safeguarding FTI when its accessed through remote workers from home. Could the IRS discuss specific rules with respect to workers, equipment use, and data transmissions to remote worksites? This information would assist our agency in determining if we would allow FTI to be accessed remotely and to formalizing our policy.

**What are the most common errors found by the IRS during inspections of states that have a sharing agreement with the IRS?**

**Does the IRS (or FTA) have a training video that will suffice for the annual recertification training requirement?**