

Office of Safeguards

Publication 1075 Updates

2014

WSATA

Conference



Internal Revenue Service

Overview

- ▶ Welcome to Safeguards (aka: Pub 1075 101)
- ▶ Emerging Issues
- ▶ Questions and Open Discussion



The ALL new Pub. 1075!



- ▶ Effective January 2014, the revised version of Publication 1075 supersedes previous versions
- ▶ The changes are extensive and incorporate feedback from stakeholders including agencies, organizations and IRS partners
- ▶ Electronically formatted for improved navigation (hyperlinks)
- ▶ Simplified language, key definitions, clarified requirements
- ▶ Added index and quick reference charts
- ▶ Feedback welcomed at: SafeguardReports@irs.gov
- ▶ Publication 1075 Link: www.irs.gov/pub/irs-pdf/p1075.pdf



What's New?

- ▶ MOST IMPORTANT: **Cover Color!!**
- ▶ Electronic only format
- ▶ Highlights page for quick summary of updates
- ▶ Simplified Minimum Protection Standards
- ▶ Index section
- ▶ Reporting requirements
- ▶ Computer Security updates
- ▶ And the list goes on and on.....



Record Keeping (Section 3.0)

- Requirements for tracking electronic and non-electronic FTI have been combined
- Examples of potential tracking elements provided

Electronic Record Keeping Log								
Date Received	Control Number/File Name	Content (do not include FTI)	Recipient/Title Location	Number of Records	Movement Date	Recipient/Title Location	Disposition Date	Disposition Method

Non-Electronic Record Keeping Log									
Date Requested	Date Received	Taxpayer Name	Tax Year(s)	Type of Information	Reason for Request	Exact Location	Who has access?	Disposition Date	Disposition Method



Secure Storage (Section 4.0)

➤ Minimum Protection Standards Simplified

Secured Perimeter	The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
Security Room	A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection, and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room.
Badged Employee	During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed and worn above the waist.
Security Container	A security container is a storage device (e.g., turtle case, safe/vault) with a resistance to forced penetration, with a security lock with controlled access to keys or combinations.



Training



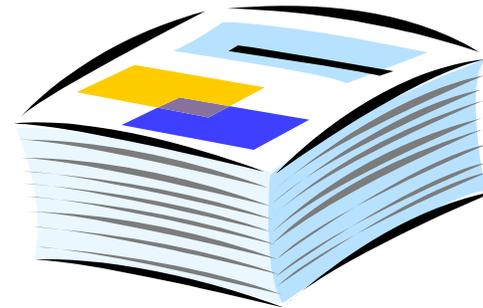
(Section 6.0)

Training Component	Applicability	Section
Disclosure Awareness Training	<ul style="list-style-type: none">• Unique to protection of FTI and prevention of unauthorized disclosure	6.3
Security Awareness Training	<ul style="list-style-type: none">• Provide basic security awareness training to information system users	9.3.2.2
Role-Based Training	<ul style="list-style-type: none">• Provides individualized training to personnel based on assigned security roles and responsibilities	9.3.2.3
Contingency Training	<ul style="list-style-type: none">• Provides individualized training to personnel based on assigned roles and responsibilities as they relate to recovery of backup copies of FTI	9.3.6.3
Incident Response Training	<ul style="list-style-type: none">• Provides individuals with agency-specific procedures to handle incidents• Provides individuals with IRS-specific requirements pertaining to incidents involving FTI	9.3.8.2 and 10.0



Reporting Requirements (Section 7.0)

- Eliminated reporting by 50%
- SAR and SPR consolidated into SSR
- SSR filed annually
- Changed SSR and CAP due dates according to state instead of agency type
- 45 Day Notification Listing



Reduced Reporting Requirements

- ▶ Effective 2014, Office of Safeguards implemented the Safeguards Security Report (SSR) as the primary source for agencies to report to IRS on the processes, procedures, and security controls in place to protect FTI provided in accordance with IRC 6103(p)(4)
- ▶ The SSR is replaced the Safeguard Procedures Report (SPR) and Safeguard Activity Report (SAR)
- ▶ *Annual* review of all security controls instead of every six years
 - Enhance the documentation and reporting of the security controls in place to protect FTI
 - Planned changes can be captured in annual report submissions eliminating the need for report addendums
- ▶ Prepare agencies for onsite reviews and enhance continuous monitoring capabilities through a regular review of implemented security controls and requirements at the agency level
- ▶ Minimize redundant documentation and reporting efforts
 - One all encompassing report instead of two reports with redundant information



CAP Submission Schedule first year.....

	Reporting Period	SSR Due
Federal Agencies		
All Federal Agencies	January 1 through December 31	January 31 2014 only: March 15
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 1 through January 31	February 28 2014 only: March 30
CNMI, CO CT DC, DE, FL, GA	March 1 through February 28	March 31 2014 only: April 15
GU, HI, IA, ID, IL, IN, KS	April 1 through March 31	April 30
KY, LA, MA, MD, ME, MI	May 1 through April 30	May 30
MN, MO, MS, MT, NE	June 1 through May 31	June 30
NC, NH, NJ, NM, NV, NY	July 1 through June 30	July 31
ND, OH, OK, OR	August 1 through July 31	August 31
PA, PR, RI, SC, SD, TN	September 1 through August 31	September 30
TX, UT, VA, VI, VT, WA	October 1 through September 30	October 31
WI, WV, WY	November 1 through October 31	November 30



	CAP with SSR	CAP (only)
Federal Agencies		
All Federal Agencies	January 31	July 31
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 28	August 31
CNMI, CO CT DC, DE, FL, GA	March 31	September 30
GU, HI, IA, ID, IL, IN, KS	April 30	October 31
KY, LA, MA, MD, ME, MI	May 30	November 30
MN, MO, MS, MT, NE	June 30	December 31
NC, NH, NJ, NM, NV, NY	July 31	January 31
ND, OH, OK, OR	August 31	February 28
PA, PR, RI, SC, SD, TN	September 30	March 31
TX, UT, VA, VI, VT, WA	October 31	April 30
WI, WV, WY	November 30	May 30



45 Day Notification Reporting Requirements

- ▶ Cloud computing
- ▶ Consolidated data center
- ▶ Contractor access
- ▶ Data warehouse processing
- ▶ Non-agency-owned information systems
- ▶ Tax modeling
- ▶ Test environment
- ▶ Virtualization of IT systems

Notification is also required for contractors to perform statistical analysis, tax modeling, or revenue projections (see Section 2.4, State Tax Agency Limitations).



Disposing of FTI (Section 8.0)



Burning

The material is to be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.

Shredding

To make reconstruction more difficult:

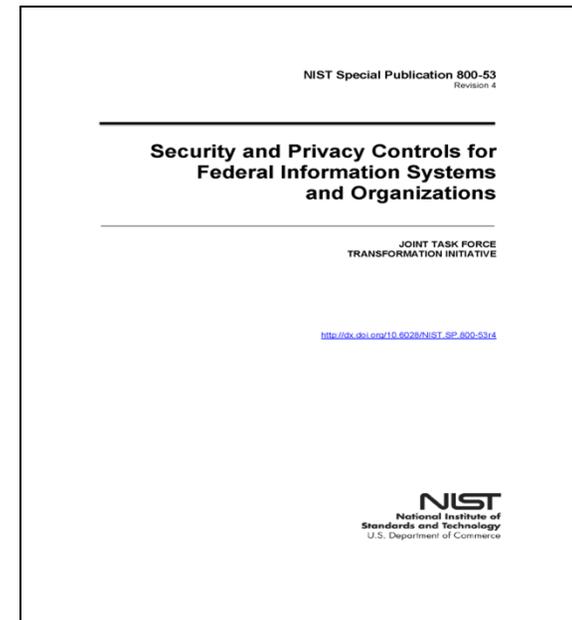
- The paper must be inserted so that lines of print are perpendicular to the cutting line.
- The paper must be shredded to effect 5/16-inch-wide or smaller strips. Consideration should be given to the purchase of cross-cut shredders when replacing or purchasing new equipment.

If shredding deviates from the 5/16-inch specification, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.



Computer Security (Section 9.0)

- ▶ Updated to meet NIST 800-53 Revision 4 requirements
- ▶ Clarified assessment process in a new Section 9.2
- ▶ Clarified encryption requirements for FTI in transit
- ▶ Added media sanitation exhibit



Computer Security (Section 9.0)

Computer security requirements detailed:

- a) Cloud computing
- b) Media sanitation
- c) Mobile devices
- d) Network protections
- e) Storage area networks
- f) System component inventory
- g) Virtual desktop infrastructure
- h) Virtualization
- i) VoIP
- j) Web-based systems and Web browsers
- k) Wireless networks



Reporting Data Incidents - TIGTA

(Section 10.0)

Field Division	Field Division Service Locations	Telephone
Atlanta	Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Mississippi, Arkansas, Puerto Rico, and U.S. Virgin Islands	404-338-7449
Chicago	Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, North Dakota, South Dakota, Wisconsin, and Ohio	312-554-8751
Dallas	Oklahoma, Texas, Louisiana, Kansas, Missouri, Nebraska	713-209-3711
Denver	Alaska, Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming	303-291-6102
New York	Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont	917-408-5681
San Francisco	California, Hawaii	510-637-2558
Washington	New Jersey, Delaware, Pennsylvania, West Virginia, Virginia, Maryland, and Washington, D.C.	267-941-3092
Internal Affairs Division	Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	202-927-7197



Conclusion

- ▶ Feedback is highly encouraged
- ▶ Please send your comments, feedback, questions to SafeguardReports@irs.gov
- ▶ Next revision in process now and expected to be released around the end of the year
- ▶ <http://www.irs.gov/pub/irs-pdf/p1075.pdf>



Questions

