Safeguard Disclosure Security Evaluation Matrix (SDSEM)

Release v1.0

September 12, 2008

Agency: *Insert agency name and type*
DES: *Insert name of DES who completed the review*
Date: *Insert date(s) review occurred*
Location: *Insert Location review was conducted, i.e., data center, field office, alternate storage site*
Agency POC(s): *Insert agency interviewee(s) name, title*

Instructions for Completing the SDSEM

Agency Instructions:
Upon receipt of the SDSEM the agency point of contact(s) should begin to complete Column I "Comments/Supporting Evidence" of the Test Case tab prior to the start of the Safeguard Review. This information will serve as evidence for the determination of the test result for each test case. The IRS Disclosure Enforcement Specialist (DES) will determine the test result for each test case based on a verification of the evidence during the Safeguard Review. The pre-populated SDSEM should be provided by the agency to the DES during the Safeguard Review kick-off on the first day of the review.

IRS Safeguards DES Reviewer Instructions:
The DES is to execute the test cases in the Test Case tab and document the results. The DES is required to complete the following columns: Column I "Pass/Fail", and Column J "Comments/Supporting Evidence." See the Legend tab for information on completing these columns.
DES # - Column B: This is an optional column not required to be completed as part of the Safeguard review. The purpose of this column is to allow the DES to customize the Test Cases tab by sorting the order of the test cases within each IRC Category to fit the individual DES's normal order of test execution while on-site. The following steps provide guidance to do this for IRC Section 6103(p)(4)(A) as an example: 1. Insert a sequence number in Column B for each test case. This is the seqence in which you will execute each test within the section. 2. Select the area to be sorted, in this case rows 3-36, columns A-J for each row. 3. Go to "Data" --> "Sort" 4. In the Sort dialog box, the Sort By drop down box reads Column B (to ensure it will sort on the DES #) and the Ascending button is selected. 5. Click OK. 6. The rows will rearrange based on the numerical order of the DES # column. 7. To undo the sort, repeat #2, 3 and 4, but ensure the Sort By drop down box reads Column A (to sort on Test ID) and click OK. **Note:** This must be done one section at a time. The gray IRC section headers cannot be selected as part of the area to sort or else the sort will not function properly.
Pass/Fail - Column I: Determine if the supporting evidence supports a Pass, Fail or N/A test result. If the control is marked as N/A, provide appropriate justification as to why the control is considered N/A. The cell will only accept the values P, F, or N/A.

Comments/Supporting Evidence - Column J: Include a supporting narrative that explains the evidence used to confirm if the test case passed, failed or is not applicable As evidence, at a minimum provide the following information for the following assessment methods:
1. Interview - Name and title of the person providing information. Also provide the date when the information is provided.
2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible).
3. Test - Provide a description of the condition observed during the test and the name and title of the agency person that assisted with the test execution.

Test ID	DES #	PUB 1075 Reporting Category	PUB 1075 REF	**NIST ID**	Test Objective	Test Steps	Assessment Method	Pass / Fail	**Comments/Supporting Evidence**
IRC Section 6103(p)(4)(A)									
1		Record Keeping Requirements	3.0	PE-16	Obtaining FTI	How is FTI received (i.e., FedEx, UPS, USPO, Secure Data Transfer, i.e., Tumbleweed, ConnectDirect, encrypted CD)?	Interview		
2		Record Keeping Requirements	3.0	PE-16	Obtaining FTI	Is FTI receipt acknowledged and returned to IRS? Is receipt logged by the agency?	Examine		
3		Record Keeping Requirements	3.0	PE-16	Obtaining FTI: Mailroom	If FTI is received through the mailroom? -Does Mailroom acknowledge receipt? -Does Mailroom log in package? -Does Mailroom bring package to another function? -Does other function sign Mailroom log?	Interview/ Examine		
4		Record Keeping Requirements	3.0	MP-2	Request for FTI	How are requests for FTI logged (Form 8796, TDS, ad-hoc requests)? Are requests compliant with IRS Publication 1075 Section 3?	Interview		
5		Record Keeping Requirements	3.0	MP-2	Request for FTI	What products or documents are created from the FTI data (e.g., letters, reports, etc.)?			
6		Record Keeping Requirements	3.0	MP-2	Request for FTI	With whom are FTI based prodcuts shared? Are logs kept?			
7		Record Keeping Requirements	3.0	MP-5	Electronic Media Containing FTI Processed	How is electronic media distributed upon receipt?	Interview		
8		Record Keeping Requirements	3.0	MP-6	Electronic Media Containing FTI Processed	What electronic media do you still have and how are you planning disposal?	Interview		

9		Record Keeping Requirements	3.0	MP-5	Electronic Media Containing FTI Processed	Is electronic media provided to a contracted State Agency or Contractor?	Interview		
10		Record Keeping Requirements	3.0	MP-5	Electronic Media Containing FTI Processed	What safeguard controls are in place when transmitting and processing electronic media at a contracted state agency or contractor site?	Interview		
11		Record Keeping Requirements	3.0	MP-2	Receipt FTI Paper Reports	List of functions in receipt of paper FTI: _____ _____ _____	Interview/ Examine		
12		Record Keeping Requirements	3.0	MP-4	Storage of IRS FTI electronic media	Where is electronic media stored before and after processing? -At Agency? -At Data Center? -Is electronic media with FTI stored with other Agency data?	Interview		
13		Record Keeping Requirements	3.2	MP-2	Electronic Files	Is a log kept or are transmittal documents retained? Documented receipt? Informal receipt? By whom? -In-house? -Contractor? -Outside of Agency?	Interview/ Examine		
14		Record Keeping Requirements	3.2	MP-2	Electronic Files	Are Electronic Media inventories performed -- Periodic? Results of prior inventories?	Examine		
15		Record Keeping Requirements	5.6.16	SI-12	Stored in the Media Library: Electronic Media Library: Procedures - File Retention Cycles	Are cycles documented and monitored to ensure destruction?	Examine		

16		Record Keeping Requirements	5.6.6	CP-9	Stored in the Media Library: Electronic Media Library: Procedures - Data Backup	How are data files backed up, by whom, and on what type of media (e.g., data center backup, agency programmer backup)?	Interview		
17		Record Keeping Requirements	5.6.16	SI-12	Stored in the Media Library: Electronic Media Library: Procedures - Retention	What is retention period of backup media and how many generations of backup files exist at the same time?	Interview		
18		Record Keeping Requirements	5.6.6	CP-6 MP-4	Stored in the Media Library: Electronic Media Library: Procedures - Retention	Where are backup files stored? Are backup files stored off-site? If so, where?	Interview/ Examine		
19		Record Keeping Requirements	5.6.6	CP-6 MP-4	Stored in the Media Library: Electronic Media Library: Procedures - Retention	How are files protected? Who has access to these files?	Interview/ Examine		
IRC Section 6103(p)(4)(B)									
20		Secure Storage	4.3.2 4.3.4	PE-3	Guards	Guards: Contract/Employee?	Interview		
21		Secure Storage	4.3.2 4.3.4	PE-3	Guards	Guards: How many posts: -Main Entrance_____ -Rear Entrance_____ -Side Entrance_____ -Outside_____ -Inside_____	Examine		
22		Secure Storage	4.3.2 4.3.4	PE-3	Guards	Guards: Hours on Duty?	Interview		

23		Secure Storage	4.3.12	PE-6	Alarms	Electronic Intrusion Alarm System?	Interview/ Examine		
24		Secure Storage	4.3.12	PE-6	Alarms	Motion Detectors?	Interview/ Examine		
25		Secure Storage	4.3.12	PE-6	Alarms	Emergency Exit Alarm?	Interview/ Examine		
26		Secure Storage	4.3.12	PE-6	Alarms	Who monitors the various alarms?	Interview		
27		Secure Storage	4.3.2	PE-6	Cameras (Outside/Inside)	Where are they placed?	Examine		
28		Secure Storage	4.3.2	PE-6	Cameras (Outside/Inside)	How many cameras?	Examine		
29		Secure Storage	4.3.2	PE-6	Cameras (Outside/Inside)	Who monitors the various cameras?	Interview		
30		Secure Storage	4.3.2	PE-6	Cameras (Outside/Inside)	Are cameras recording their view?	Test		
31		Secure Storage	4.3.2	PE-6	Cameras (Outside/Inside)	How long are electronic medias maintained?	Interview/ Examine		
32		Secure Storage	4.3.2	PE-6	Access: Monitoring	Who monitors access control?	Interview		
33		Secure Storage	4.3.2	PE-6	Access: Monitoring	How often is access control monitored?	Interview		
34		Secure Storage	4.3.2	PE-2	Access: Keys/Cards	What is used to control access from the **outside:** Keys or Electronic access control system?	Examine/ Test		
35		Secure Storage	4.3.10 4.3.11	PE-2	Access: Keys/Cards	What is used to control access from the **inside:** Keys or Electronic access control system?	Examine/ Test		
36		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Is a record maintained on the issuance of keys/key cards? Buildings: Offices: Containers:	Examine		

37		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	If so, how are records maintained (i.e., custody receipt/automated file)? Buildings: Offices: Containers:	Examine		
38		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Who is responsible for issuance of keys/key cards? Buildings: Offices: Containers:	Interview		
39		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Who has access to keys/key cards? Buildings: Offices: Containers:	Interview		
40		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Are periodic reviews being conducted to reconcile records? Buildings: Offices: Containers: When was the last review?	Interview/ Examine		
41		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Is there a written policy on recovery of ID/keys/key cards after employee leaves?	Examine		
42		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Is the locking mechanism checked? Buildings: Offices: Containers: How often?	Interview		

43		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Who controls the duplicate keys for: Buildings: Offices: Containers:	Interview		
44		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Are all employees given keys to: Buildings: Offices: Containers:	Interview		
45		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	What is the key reproducing policy? Buildings: Offices: Containers:	Interview/ Examine		
46		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Who maintains the key to cabinet that contain(s) the IRS electronic media?	Interview		
47		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Where is the key kept during the day?	Interview/ Examine		
48		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Where is the key kept at night?	Interview/ Examine		
49		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	Who maintains backup keys to cabinets that contain the IRS electronic media(s) or FTI Reports?	Interview		
50		Secure Storage	4.3.10	PE-2	Access: Keys/Cards	How many keys are there in total?	Interview		
51		Secure Storage	4.3.10	PE-3	Access: Combinations	How often are door/safe combinations changed?	Interview		
52		Secure Storage	4.3.10	PE-3	Access: Combinations	Who is responsible to change the combinations?	Interview		
53		Secure Storage	4.3.10	PE-3	Access: Combinations	Who has access to combinations?	Interview		
54		Secure Storage	4.3.10	PE-3	Access: Combinations	Who controls (records)/safeguards combinations?	Interview		
55		Secure Storage	4.3.10	PE-3	Access: Combinations	How are combinations safeguarded?	Interview		

56		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	Are employees wearing the agency authorized IDs?	Test		
57		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	Are lost ID cards reported?	Interview		
58		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	How do employees enter the work area without an ID card?	Interview		
59		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	Is there a written policy on ID cards?	Examine		
60		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	Are ID cards inventoried (i.e., automated, written down and placed in safe, etc.)?	Examine		
61		Secure Storage	4.3.2	PE-2	ID Cards (Badges)	Who has access to ID Card/Badge inventory?	Interview		
62		Secure Storage	4.3.2	PE-7	Visitor/Vendor Access	Do visitors/vendors sign a visitor access log?	Examine		
63		Secure Storage	4.3.2	PE-8	Visitor/Vendor Access	Does the visitor access log contain the following information? (i) name and organization of the visitor; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited.	Examine		
64		Secure Storage	4.3.2	PE-8	Visitor/Vendor Access	Do designated officials or designees within the agency review the visitor access records, at least annually?	Interview		
65		Secure Storage	4.3.2	PE-7	Visitor/Vendor Access	Are visitors/vendors escorted?	Interview/ Examine		

66		Secure Storage	4.3.2	PE-7	Visitor/Vendor Access	Are visitors/vendors issued ID cards? Are ID cards turned in at end of day? Are ID cards inventoried/monitored?	Interview/ Examine		
67		Secure Storage	4.3.1	PE-3	Restricted Area	Verify two barriers are present to access FTI under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container.	Examine		
68		Secure Storage	4.3.1	PE-3	Restricted Area	Specify the Restricted Access areas (i.e., Cashier, Filing Room, Mailroom, Work Areas) where FTI is located?	Interview/ Examine		
69		Secure Storage	4.3.1	PE-2	Restricted Area	Who authorizes access?	Interview		
70		Secure Storage	4.3.1	PE-2	Restricted Area	Are the names of departed/transferred employees removed? When are they removed?	Interview/ Examine		
71		Secure Storage	4.3.1	PE-2	Restricted Area	Is an access record review conducted to update who can access certain areas? How often?	Interview		
72		Secure Storage	4.3.1	PE-6	Restricted Area	Who reviews electronic and paper audit trails? How often are they reviewed?	Interview		
73		Secure Storage	4.3.1	PE-3	Restricted Area	How is access restricted?	Interview		
74		Secure Storage	4.3.1	PE-3	Restricted Area	How is area secured?	Interview/ Examine		
75		Secure Storage	4.3.1	PE-6	Restricted Area	What controls are in place to monitor access to restricted area (i.e., logs, electronic monitoring)?	Interview/ Examine		
76		Secure Storage	4.5	PE-16	Loading Docks	How are loading docks secured?	Interview/ Examine		
77		Secure Storage	4.5	MP-4	Document Security	Provide a description of the types of FTI maintained at the work area.	Interview		
78		Secure Storage	4.36 4.37 4.38	MP-4	Document Security	Is FTI maintained in container commensurate with level of sensitivity?	Examine		

79		Secure Storage	4.5	MP-4	Document Security	Are documents containing FTI stored in a locked container until pick-up for disposal?	Examine		
80		Secure Storage	4.5	MP-5	Document Security	How is the paper waste material transported?	Interview		
81		Secure Storage	4.3.4	MP-2	Document Security	Is there a “clean desk” policy (should cover desktop, credenzas, and in/out baskets)? Is it in writing?	Examine		
82		Secure Storage	4.3.4	MP-2	Document Security	Does management periodically conduct an after-hours check to ensure the clean desk policy, i.e., locked containers, office doors locked, etc. How often? When was the last review? Were there any findings and have there been any findings and corrective actions taken?	Interview/ Examine		
83		Secure Storage	4.36 4.37 4.38	MP-4	Containers	What type of container is used to store FTI (i.e., lateral, upright, credenza, overhead, desk, safes, vaults)?	Examine		
84		Secure Storage	4.36 4.37 4.38	MP-4	Containers	Do all containers have locks?	Examine		
85		Secure Storage	4.3.9	MP-4	Containers	What type of lock (i.e., lock bars, key lock, padlock, combination padlock)?	Examine		
86		Secure Storage	4.36 4.37 4.38	MP-4	Containers	Is FTI containerized after hours or when not in the custody of agency employees?	Interview/ Examine		
87		Secure Storage	4.36 4.37 4.38	MP-4	Containers	Are containers locked after hours?	Interview/ Examine		
88		Secure Storage	4.3.4	PE-3	Office Security	Are office doors locked after hours?	Interview/ Examine		
89		Secure Storage	4.3.4	PE-3	Office Security	How is access restricted to offices?	Interview/ Examine		

90		Secure Storage	4.3.4	PE-2	Office Security	Who has access to the offices after hours? Cleaning Crews: Landlord: Maintenance Crews: Security Guards: Employees (i.e. all or management):	Interview		
91		Secure Storage	4.3.4	MP-2	File Rooms Containing FTI	Does file room have its own staff? How many employees?	Interview		
92		Secure Storage	4.3.4	MP-2	File Rooms Containing FTI	Can only file room staff access client files?	Interview		
93		Secure Storage	4.3.4	MP-5	File Rooms Containing FTI	Are removal/returns logged/scanned?	Examine		
94		Secure Storage	4.3.4	MP-4	File Rooms Containing FTI	Is there a follow-up for missing files performed?	Interview		
95		Secure Storage	4.3.4	MP-4	File Rooms Containing FTI	Is file room door locked at night?	Interview/ Examine		
96		Secure Storage	4.3.4	MP-2	File Rooms Containing FTI	If so, who can access the room after normal working hours (i.e., cleaning, guards, maintenance)?	Interview		
97		Secure Storage	4.3.4	MP-4	Storage of Files Containing FTI	Are files stored at the field office/district office/Agency?	Interview/ Examine		
98		Secure Storage	4.3.4	MP-4	Storage of Files Containing FTI	How long are files stored at the field office/district office/Agency?	Interview		
99		Secure Storage	5.6.6	CP-6	Storage Off-Site	Are files stored at a alternate storage facility?	Interview		
100		Secure Storage	5.6.6	CP-6	Storage Off-Site	If this is a Agency facility, do Agency employees work at the facility?	Interview		
101		Secure Storage	5.6.6	CP-6	Storage Off-Site	If this is a Contractor Facility, how is access limited to non-agency employees?	Interview		
102		Secure Storage	4.5 5.6.6	CP-6 MP-5	Storage Off-Site	How are they shipped / transfer to alternate storage facility)?	Interview		
103		Secure Storage	4.5 5.6.6	CP-6 MP-5	Storage Off-Site	What type of container is used to ship the files?	Interview/ Examine		

104		Secure Storage	4.5 5.6.6	CP-6 MP-5	Storage Off-Site	Is the container taped or locked?	Examine/ Test		
105		Secure Storage	4.5 5.6.6	CP-6 MP-5	Storage Off-Site	For retrieval of case file, is entire container recalled, or is file recalled?	Interview		
106		Secure Storage	4.5 5.6.6	CP-6 MP-5	Storage Off-Site	Who is in charge of storage or shipping files to storage facilities?	Interview		
107		Secure Storage	5.6.6	CP-6 MP-2	Storage of Files Containing FTI	Does the storage contractor sub-contract FTI out?	Interview		
108		Secure Storage	5.6.16	SI-12	Storage of Files Containing FTI	Is there a written policy on document retention?	Examine		
109		Secure Storage	5.6.16	SI-12	Storage of Files Containing FTI	Does the agency retain output from the system that includes FTI in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to, special instructions for dissemination, distribution, transport, or storage of information system output?	Examine		
110		Secure Storage	4.7	PE-17	Alternate Work Site	Are employees allowed to work with FTI from an alternate work site (i.e., any working area that is attached to the Wide Area Network (WAN) either through a Public Switched Data Network (PSDN) or through the Internet)?	Interview/ Examine		
111		Secure Storage	4.7	PE-17	Alternate Work Site	Does the agency have a documented plan for the security of alternative work site?	Examine		

112		Secure Storage	4.7	PE-17	Alternate Work Site	Does the agency certify the security controls of the alternate work site are adequate for security needs. Additionally, does the agency promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules should address brief absences while employees are away from the computer.	Examine		
113		Secure Storage	4.7	PE-17	Alternate Work Site	Do all computers and mobile devices that contain FTI and are resident in an alternate work site employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost and/or stolen? What is the encryption strength?	Examine/ Test		
114		Secure Storage	4.7	PE-17	Alternate Work Site	Does the agency provide specialized training in security, disclosure awareness, and ethics for all participating employees and managers? Does the training cover situations that could occur as the result of an interruption of work by family, friends, or other sources?	Interview/ Examine		
115		Secure Storage	4.7	PE-17	Alternate Work Site	Does the agency conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. Are the results of each inspection documented?	Interview/ Examine		
116		Secure Storage	4.7	PE-17	Alternate Work Site	Does the agency retain ownership and control, for all hardware, software, and telecommunications equipment connecting to public communication networks, where these are resident at all alternate work sites.	Interview		

117		Secure Storage		CP-7	Alternate Processing Site	Does the agency have an alternate site identified for business resumption when the primary processing location (office space) is unavailable? The alternate site could be a (i) dedicated site owned or operated by the agency, (ii) reciprocal agreement or memorandum of agreement with an internal or external entity, or (iii) commercially leased facility.	Interview/ Examine		
118		Secure Storage		CP-7	Alternate Processing Site	Does the agency have an alternate processing site agreement in place to permit the resumption of operations? Does the agreement define the time period within which processing must be resumed at the alternate processing site?	Examine		
119		Secure Storage	4.3.2	PE-5	Access Control for Display Medium	Are computer monitors or other display devices that display FTI positioned so as to not be visible to passers-by in hallways or common areas?	Examine		
120		Secure Storage	4.32 4.33 4.34	PE-18	Location of Information System Components	For all areas that process FTI, does the agency position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access?	Examine		
121		Secure Storage	4.4	PE-3	Security During Office Moves	How is FTI protected during an office move? Is FTI kept in locked cabinets or sealed packing cartons during the move?	Interview		
IRC Section 6103(p)(4)(C)									
122		Restricting Access	5.3	MP-2	Commingling	How is FTI filed?	Interview		
123		Restricting Access	5.3	MP-2	Commingling	How can FTI be retrieved?	Interview		

124		Restricting Access	5.3	MP-2	Commingling	What identifying information is used for retrieval? Individual name?	Interview		
125		Restricting Access	5.3	MP-2	Commingling	Is FTI kept separate or commingled with other information?	Interview/ Examine		
126		Restricting Access	5.3	MP-2	Commingling	If commingled, is commingled FTI identifiable?	Interview/ Examine		
127		Restricting Access	5.3	MP-2	Commingling	Can FTI within agency records be located and segregated?	Interview		
128		Restricting Access	5.3	MP-2	Commingling	Please provide letters (Verification, Adjustment, Third Party) used to obtain FTI verification from clients, financial institutions and others.	Examine		
129		Restricting Access	5.3	MP-2	Commingling	What specific data, from FTI, is entered into the system after independent verification has been received?	Interview		
130		Restricting Access	11.0 11.4	MP-2 SA-9	Contractor Access	Is data disclosed to any contractor? Identify the data disclosed to the contractor.	Interview/ Examine		
131		Restricting Access	11.0 11.4	MP-2 SA-9	Contractor Access	Provide a copy of the contractor's contract.	Examine		
132		Restricting Access	11.0 11.4	MP-2 SA-9	Contractor Access	Does the contract include the required Safeguards language in the contract?	Examine		
133		Restricting Access	11.0 11.4	MP-2 SA-9	Contractor Access	Does the contractor sub-contract any work containing FTI?	Interview		
134		Restricting Access	11.0 11.4	SA-9	External Information System Services	Does the agency outsource information system services for systems that store, process or transmit FTI to provider external to the agency (contractor)? Does the contract include the required Safeguards language in the contract?	Interview/ Examine		
135		Restricting Access	5.2	AC-6	Access	How is access limited to authorized employees?	Interview		
136		Restricting Access	5.2	AC-6	Access	Who designates authorized employees?	Interview		

137		Restricting Access	5.2	AC-6	Access	Do all authorized employees have a need-to-know?	Interview		
138		Restricting Access	5.2	AC-6	Access	Do Auditors have access to case files?	Interview		
139		Restricting Access	5.2	AC-6	Access	Are disclosures of FTI made to congresspersons on behalf of their constituents?	Interview		
140		Restricting Access	5.2	AC-6	Access	Provide the written procedures in effect for specifying to whom disclosures of FTI can be made.	Examine		
141		Restricting Access	5.2	AC-6	Quality Control/Quality Assurance/Quality Review	Do reviewers have access to FTI online? In paper?	Test		
142		Restricting Access	5.2	AC-6	Quality Control/Quality Assurance/Quality Review	Do reviewers send out verification letters on FTI?	Interview		
143		Restricting Access	5.2	AC-6	Quality Control/Quality Assurance/Quality Review	Are reviewers agency employees?	Interview		
144		Restricting Access	5.2	AC-6	Other Entities	Do other entities (e.g., volunteers, researchers, contractors, non-agency employees) have access to FTI?	Interview		
145		Restricting Access		AC-6	Federal Offset Payments	Are Federal Offset Payments released to courts or other third parties, such as custodial parents?	Interview		
146		Restricting Access		AC-6	Federal Offset Payments	Does the agency receive Federal Offset Payments (Applies to Revenue and Child Support)?	Interview		
147		Restricting Access		AC-6	Federal Offset Payments	Does the agency use a contractor to process the Offset (Reconciliation of payment or data processing)?	Interview		
148		Restricting Access	5.4	AC-6	Sharing FTI	Is FTI shared between Child Support, Welfare or Labor? Are employees shared between these agencies?	Interview		

149		Restricting Access	5.4	AC-6	Sharing FTI	Does the agency share FTI with any agency or entity e.g. tribes, cities/states, other state agencies)? If yes, by what authority?	Interview		
150		Restricting Access	5.2	AC-6	Modeling	Does the agency use FTI for modeling and or revenue projections? If yes, do they have a current need and use statement?	Interview/ Examine		
151		Restricting Access	5.2	AC-6	Portal Access	Does the agency have internal or external facing web applications or portals? Is FTI accessible through the portal/web applications? Who has access?	Interview/ Test		
152		Restricting Access	5.6.1	AC-6	Web Based Access	Does the agency have web based applications?	Interview		
153		Restricting Access	5.6.1	AC-6	Web Based Access	Is FTI accessible through the web site? Who has access to web site?	Test		
154		Restricting Access		AC-6	Client Representation	Who can represent a client?	Interview		
155		Restricting Access	5.5	AC-6	Computer Center Facility	If this is an Agency facility, who works at the facility? -Only agency employees? -Computer programmers? -How is access to FTI limited to contractors?	Interview		
156		Restricting Access	5.6.2	AU-2	FTI Access Logs	What information is available on the FTI access log reports?	Examine		
157		Restricting Access	5.6.2	AU-6	FTI Access Logs	Are FTI access log reports monitored to detect unauthorized browsing?	Interview		
158		Restricting Access	5.6.2	AU-6	FTI Access Logs	What actions are taken when unauthorized action is found on an FTI access log report?	Interview		
159		Restricting Access	5.6.2	AU-2	FTI Access Logs	Are FTI access logs maintained of accesses or updates to electronic data?	Test		
160		Restricting Access	5.6.2	AU-2	FTI Access Logs	Are access records or listings of FTI extracts made?	Test		

161		Restricting Access	5.6.2	AU-2	FTI Access Logs	Do these FTI access logs include: -Reason for access? -Current location of data? -Final disposition? -Who monitors? -How often monitored? -Any findings within the last two years? -What action was taken?	Test		
162		Restricting Access		PS-1	Personnel Security Policy and Procedures	Does the agency have a personnel security policy that addresses position categorization, personnel screening, personnel termination, personnel transfer, and access agreements?	Examine		
163		Restricting Access		PS-1	Personnel Security Policy and Procedures	Does the agency have personnel security procedures that address the policy elements and is disseminated to employees responsible for implementing personnel security?	Examine		
164		Restricting Access	5.17.6.5	-	Electronic Mail	Does the agency have a policy that states FTI shall not be transmitted or used on email systems?	Examine		
165		Restricting Access	5.17.6.5	-	Electronic Mail	If it is necessary to transmit FTI via email, does the agency take the following precautions to protect FTI sent via email? -FTI is encrypted in the email -Attachments containing FTI are encrypted -Ensure that all messages sent are to the proper address, and -Employees should log off the computer when away from the area.	Interview		

166		Restricting Access	5.17.6.6	-	Fax Machines	If FAX machines are used to transmit FTI does the agency take the following precautions to protect Fax transmissions? -A trusted staff member is located at both the sending and receiving fax machines. -Broadcast lists and other preset numbers of frequent recipients of FTI are maintained and periodically updated -Fax machines are placed in a secured area. -A cover sheet is included on fax transmissions that explicitly provides guidance to the recipient, which includes: -A notification of the sensitivity of the data and the need for protection -A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information.	Interview/ Examine		
IRC Section 6103(p)(4)(D)									
167		Other Safeguards	6.2	AT-1	Employee Awareness	Does the agency have a security awareness and training policy?	Examine		
168		Other Safeguards	6.2	AT-1	Employee Awareness	Does the agency have security training and awareness procedures that address the policy elements and is disseminated to employees responsible for implementing security training and awareness?	Examine		
169		Other Safeguards	6.2	AT-2	Employee Awareness	Are new employees given a security orientation prior to having access to FTI?	Interview		

170		Other Safeguards	6.2	AT-2	Employee Awareness	Does the orientation cover FTI?	Examine		
171		Other Safeguards	6.2	AT-2	Employee Awareness	Does the orientation cover Penalty Provisions under the Internal Revenue Code (IRC) 7213, 7213A and 7431?	Examine		
172		Other Safeguards	6.2	AT-2	Employee Awareness	Do employees sign a certification at initial security awareness orientation (provide a copy of agreement)?	Examine		
173		Other Safeguards	6.2	AT-2	Employee Awareness	Do employees sign a re-certification every year thereafter?	Test		
174		Other Safeguards	6.2	AT-2	Employee Awareness	Are contractors included in the employee awareness orientation?	Interview		
175		Other Safeguards	6.2	AT-2	Employee Awareness	Does the agency maintain training records for employees/contractors that identifies the security and awareness training that each user has completed?	Examine		
176		Employee Awareness	6.2	MP-2	Document Security	Are employees aware of the need to protect FTI against inadvertent disclosure when visitors/maintenance personnel/vendors are in work area?	Interview		
177		Other Safeguards	6.3	CA-2	Internal Inspections	Is the agency periodically audited by a Third Party (e.g. Internal Audit, Inspector General (IG))?	Interview		
178		Other Safeguards	6.3	CA-2	Internal Inspections	When was the last audit conducted? Provide a copy of the audit report.	Examine		
179		Other Safeguards	6.3	CA-2	Internal Inspections	Does the agency conduct internal audit inspections of field offices that address the safeguard requirements the IRC and the IRS impose?	Interview		

180		Other Safeguards	6.3	CA-2	Internal Inspections	How often are internal inspections held for - -Field offices? -District offices? -County offices? -Central office? -Headquarters? -Administration? -Storage Facilities?	Interview		*Note: All local offices receiving FTI are reviewed within a three-year cycle. Headquarters office facilities housing FTI and the agency computer facility should be reviewed within an 18-month cycle.*
181		Other Safeguards	6.3	CA-2	Internal Inspections	Who conducts the internal inspections?	Interview		
182		Other Safeguards	6.3	CA-2	Internal Inspections	Are follow-up reviews conducted to determine the effectiveness of corrective actions taken on findings from after-hours and duty hours reviews?	Interview		
183		Other Safeguards	6.3	CA-2	Internal Inspections	During the past two inspections, were there findings? If so, what action was taken?	Interview		
184		Other Safeguards	6.3	CA-2	Internal Inspections	Are copies of the inspection report submitted with the annual SAR?	Examine		
185		Other Safeguards	6.3	CA-2	Internal Inspections	Please provide a copy of the questionnaire that is used for the internal inspection review process.	Examine		
IRC Section 6103(p)(4)(E)									
186		Reporting Requirements	7.2	PL-2	Safeguard Procedures Report	When was the last SPR submitted?	Interview/ Examine		
187		Reporting Requirements	7.2	PL-2	Safeguard Procedures Report	Have there been any significant changes since the last SPR was submitted?	Interview		
188		Reporting Requirements	7.2	PL-2	Safeguard Procedures Report	If the agency has a data warehouse is it reflected in the SPR?	Examine		
189		Reporting Requirements	7.4	PL-2	Safeguard Activity Report	When was the last SAR submitted?	Interview/ Examine		

190		Reporting Requirements	7.4	PL-2	Safeguard Activity Report	Did the last SAR include Electronic Media inventory?	Examine		
IRC Section 6103(p)(4)(F)									
191		Disposing Federal Tax Information	8.3	MP-6	Paper FTI	Is FTI paper waste material generated?	Interview		
192		Disposing Federal Tax Information	8.3	MP-6	Paper FTI	Where is paper waste material placed? -Recycle bins? -Locking container? -Waste paper basket? -Container on desk?	Examine		
193		Disposing Federal Tax Information	8.3	MP-6	Paper FTI	How is paper waste material destroyed? -Shredding (i.e., are strips rendered unreadable, size of strips, print perpendicular to cutting line)? -Pulping (i.e., what size is material reduced to) ? -Burning (i.e., is there complete combustion)? -Disintegration (how fine a screen is used)?	Interview		
194		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI	Who performs destruction of paper waste material? -Agency staff? -Contractor?	Interview		
195		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI	Who picks up/takes material for destruction? -State Agency/Federal Agency? -Contractor?	Interview		
196		Restricting Access	8.3 8.4	AC-6	Destruction Facility	If the destruction facility is a contractor facility, how is access to FTI limited to employees?	Interview		
197		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	What is the name of the contractor used for pick up and destruction of materials?	Interview		

198		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	Location of the contractor used for pick up and destruction of materials?	Interview		
199		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	Name and telephone number of contact person at the contractor used for pick up and destruction of materials?	Interview		
200		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	If the contractor does not have a destruction facility, where is the material taken?	Interview		
201		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	Does Agency staff accompany material and view destruction?	Interview		
202		Disposing Federal Tax Information	8.3 8.4	MP-6	Paper FTI: Contractor	How is material packaged when surrendered to contractor?	Interview/ Examine		
203		Disposing Federal Tax Information	8.3 8.4	MP-6	Electronic Media Library: Procedures - Destruction	Is material shredded (size of material)?	Test		
204		Disposing Federal Tax Information	8.3 8.4	MP-6	Electronic Media Library: Procedures - Destruction	Returned to the IRS? Returned to scratch pool?	Interview		
205		Disposing Federal Tax Information	8.3 8.4	MP-6	Electronic Media Library: Procedures - Destruction	What is the method for clearance of Electronic Media (removable or non-removable; e.g., primary or systemic backups) before reallocation or destruction?	Interview		
206		Disposing Federal Tax Information	8.3 8.4	MP-6	Electronic Media Library: Procedures - Destruction	Is data erased? If so, in what manner: -Degaussed (specify make and strength of degaussed)? -Written over with 0 (zero) and 1 (one)? -Written over with new data? -Written over with FTI only?	Interview		
Need and Use									

207		Need and Use	2.2	AC-6	Need and Use	For every FTI data extract received by the agency for an authorized use, does the agency have a need?	Interview		
208		Need and Use	2.2	AC-6	Need and Use	Where is the need defined? Initial agreement with IRS? Need and use statement?	Examine		
209		Need and Use	2.2	AC-6	Need and Use	Is use of the FTI documented? Examine case files for evidence.	Examine		
Incident Reporting									
210		Reporting Improper Inspections or Disclosures	10.1	IR-1	Incident Response	Is there a documented policy with steps for reporting unauthorized disclosure of FTI?	Examine		
211		Reporting Improper Inspections or Disclosures	10.1	IR-1	Incident Response	Does the incident reporting policy contain the Field Division and TIGTA contact information, coordination steps and detail when these entities should be notified of the incident?	Examine		
212		Reporting Improper Inspections or Disclosures	10.1	IR-2	Incident Response Training	Does the agency provide incident response training to personnel with incident response roles and responsibilities? Is Initial training provided, and refresher training provided at least annually?	Interview/ Examine		
213		Reporting Improper Inspections or Disclosures	10.1	IR-3	Incident Response Testing and Exercises	Does the agency test/exercise the Disclosure aspect of its incident response capability at least annually? Review documented test results of prior incident response tests.	Examine		
214		Reporting Improper Inspections or Disclosures	10.1	IR-4	Incident Handling	Does the agency's incident response procedures address an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery and post-incident activity?	Examine		

215		Reporting Improper Inspections or Disclosures	10.1	IR-5	Incident Response	Is the incident documented, tracked and monitored?	Interview/ Examine		
216		Reporting Improper Inspections or Disclosures	10.1	IR-5	Incident Response	Does the agency document the incident search efforts? Do they notify the impacted Tax Payer(s)?	Examine		
217		Reporting Improper Inspections or Disclosures	10.1	IR-6	Incident Reporting	Does the agency promptly report incident information involving a compromise of FTI to the appropriate Agent-in-Charge, TIGTA.	Interview/ Examine		
218		Reporting Improper Inspections or Disclosures	10.1	IR-7	Incident Response Assistance	Does the agency provide an incident response support resource for users? Possible implementations of incident response support resources include a help desk or an assistance group, and access to forensics services.	Interview		
Other DES Observations									
220									
221									
222									

Notes to reviewer:

IRS Safeguards SDSEM Legend	
DES #	Identification number of SCSEM test case that allows each DES to customize the SDSEM to fit the order in which the tests are actually executed on-site during a review.
Pub 1075 Reporting Category	IRC 6103 Category
Pub 1075 REF	Reference to the Section in IRS Publication 1075 where the test maps to.
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Assessment Method	The assessment methods define the nature of the actions that the assessor should take to execute the test case and obtain supporting evidence. The "Examine", "Interview" and "Test" assessment methods are used in the SDSEM. Definiton of those assessment methods is provided below: **Examine:** The process of checking, inspecting, reviewing, observing, studying, or analyzing evidence (assessment objects) to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time. Typical assessment objects for the Examine method include: Specifications (e.g., policies, plans, procedures, system requirements, designs); Mechanisms (e.g., functionality implemented in hardware, software, firmware) and Activities (e.g., system operations, administration, management; exercises). **Interview:** The process of conducting discussions with individuals or groups within an organization to facilitate support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time. Typical assessment objects for the Interview method include: Individuals or groups of individuals. **Test:** The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time. Typical assessment objects for the Test method include: Mechanisms (e.g., hardware, software, firmware) and Activities (e.g., system operations, administration, management; exercises).
Pass/Fail	Reviewer to indicate if the test case passed, failed or is not applicable. Choose from the drop down list; accepted values are "P" (pass); "F" (fail) and "N/A" (not applicable).
Comments / Supporting Evidence	Evidence to support the test result for the test case is documented here. As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the interview occurred and an indication of whether or not the information provided by the interviewee meets the test objective. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible) and an indication of how the document examined does or does not meet the test objective. 3. Test - Description of the condition observed during the test and how it does or does not meet the test objective. If the test case is marked as N/A, then provide appropriate justification as to why the control is considered N/A.