Safeguard Computer Security Evaluation Matrix (SCSEM)

Management, Operational and Technical Controls
Data Warehouse Appendix

Release IV

Version 0.1
September 18, 2008

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occurred*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

ID	Control Class	Control Family	REF. ID	Control Name	Procedures	Expected Result	Pass / Fail	Actual Results	Comments / Supporting Evidence
1	T	SC	DW-01	Data Warehouse Load	1. Determine the mechanism(s) used to input data into the data warehouse environment (e.g., A Data Warehouse is a structure that is designed to distribute data from multiple arenas to the primary enterprise system. A DW collects, extracts, transforms, transports, and loads data for a distribution. In the context of FTI within agencies, the DW stores sets of historical data, which contains specific taxpayer information, as well as summary information and historical data.) 2. Examine the controls in place to protect transmission of data into the data warehouse environment.	1. All Internet transmissions are encrypted using HTTPS protocol utilizing at least a 128 bit length key. All sessions for extract, transform and load stages of data entering a warehouse are protected with end-to-end encryption, i.e., from workstation to point of data.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*

2	O	SI	DW-02	Data Warehouse Load	1. Determine the mechanism(s) used to check data input to the data warehouse environment for completeness, accuracy and validity.	1. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. 2. Data that does not match the required format and content are rejected.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*
3	T	SI	DW-03	Data Warehouse Load	1. Examine the list of personnel authorized to input data to the data warehouse environment. 2. Verify the list of authorized personnel contains only current personnel with a job function that requires this level of access. 3. Examine the list of authorized data sources of input to the data warehouse environment (i.e., interconnected systems).	1. Only personnel with a job function that requires them to input data to the data warehouse environment have this level of access. 2. Personnel who no longer require this level of access are promptly removed from the access list. 3. Proper data sharing agreements are in place between the data source and the data warehouse environment to include mechanisms for the protection of FTI.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*

4	T	SC	DW-04	Data Warehouse Data Storage	1. Determine controls in place to protect FTI data while at rest in the data warehouse environment.	1. Database tables containing FTI are encrypted within the database. 2. Access to database tables containing FTI are restricted to authorized personnel only. 3. FTI data is not commingled with other state agency data within database tables.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*

5	T	IA	DW-05	Data Warehouse Identification & Authentication	1. Determine if access attempts to the data warehouse environment require the user to be identified and authenticated prior to access being granted. Note: There are various ways to access the data warehouse environment. Ensure identification and authentication controls are implemented for the following access mechanisms: 1) Direct access to the backend database management system and data dictionary; 2) Operating system access to the platform where the database resides; 3) Access to the application used to query the data warehouse environment and produce reports. 2. Determine if there are any automated processes that access the data warehouse for data retreival and verify the identification and authentication mechanism in place for these processes.	1. Identification and authentication is required at the operating sytsem, database and application level within the data warehouse environment. 2. Automated processes that access the data warehouse are identified and authenticated using process account credentials.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*

6	T	AC	DW-06	Data Warehouse Access Control	1. Determine who has access to the data warehouse environment from all possible connection points including: 1) Direct access to the backend database management system and data dictionary; 2) Operating system access to the platform where the database resides; 3) Access to the application used to query the data warehouse environment and produce reports.	1. Access is restricted to authorized application end users, operating system administrators and database administrators. 2. Personnel who no longer require access to the data warehouse environment are promptly removed from the access list.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*
7	T	AU	DW-06	Data Warehouse Security Auditing	1. Determine the security relevant events that are captured in the audit logs within the data warehouse environment. 2. Verify that security events are caputred in logs at the operating system, database and application level.	1. The data warehouse captures all changes made to data, including: additions, modifications, or deletions. If a query is submitted, the audit log must identify the actual query being performed, the originator of the query, and relevant time/stamp information. 2. Security events are captured in logs at the operating system, database and application level.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*

8	T	AC	DW-07	Data Warehouse Data Flow	1. Examine the flow of FTI through the data warehouse environment to verify it is properly identified as FTI at all access points, including any FTI that is included in report output.	1. In the case of a data warehouse, FTI can be commingled if the proper security controls are installed. 2. Ensure data monitoring software that can administer security down to databases, data profiles, data tables, or data columns and rows is implemented 3. Ensure the FTI within any database, data profile, data table or data column and row is back-end labeled and tagged with an IRS identifier. The same pertains to any reports generated from the data warehouse.			*Note: This test only applies if a data warehouse is currently being used by the agency to store and process/analyze FTI.*
9	T	SC	DW-08	Data Warehouse Processing	1. Examine the controls in place to protect the retreival of data from the data warehouse to be used for analysis and reporting and controls surrounding data extraction and transformation.	1. 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.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each

ID		Identification number of SCSEM test case
PUB 1075	**Control Class**	NIST 800-53/PUB 1075 Control Class (Management, Operational, Technical)
	Control Family	NIST 800-53/PUB 1075 Control Family (Risk Assessment, Security Planning, System and Services Acquisition, Security Assessment, Personnel Security, Contingency Planning, Configuration Management, System Maintenance, System and Information Integrity, Incident Response, Security
	REF. ID	NIST 800-53/PUB 1075 Reference Identification (1, 2, etc.)
Control Objective		Objective of test procedure.
Test Procedure & Expected Results		Detailed test procedures to follow for test execution, and the expected outcome of the test step
Actual Results		The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail		Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence		Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable 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 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). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.

Data Warehouse Testing Scope:	**The test cases contained in this SCSEM are meant to be an objective based test of the Data Warehouse implementation. Detailed database specific controls and secure configuration related controls are not in-scope. This appendix is only executed for data warehouse implementations.**

Version	Release Date	Summary of Changes	Changed By	Comments
0.1	9/18/2008	First Release	Jonathan Isner	