

Certification Standards (*Update 8/16/12*)SECTION I - INTRODUCTION

Article V, Section 501, of the **Streamlined Sales and Use Tax Agreement (SSUTA)**, as adopted on November 12, 2002, calls for the Governing Board of the Member States to certify automated systems and service providers to aid in the administration of sales and use tax collections that fall under the aegis of that agreement.

As an integral part of that function, the Governing Board has adopted the standards and practices found in the body of this document as the accepted measure for the certification and accountability (audit) of the Certified Service Providers (CSP) and Certified Automated Systems (CAS) as defined in Article II, Sections 202 and 203 of the SSUTA cited above.

In addition to the certification standards contained in this document, the following documents are especially important to understand up front:

- Streamlined Sales Tax Implementation Guide
- Appendix C (Minimum Standards)
- Appendix E (Testing Process for Certification of Service Providers and Automated Systems)
- Appendix F (Audit Reports)

The standards that follow, and the requirements for achieving compliance with them, are based on internal controls, security and auditing practices commonly accepted in business and government today. The following resources are available for better understanding these standards and requirements:

- The United States Government Accounting Office (GAO) “Federal Information Systems Control Audit Manual” (FISCAM), issued February 2009 (GAO-09-232G);
- National Institute of Standards and Technology (NIST) No. 53, “Recommended Security Controls for Federal Information Systems and Organizations”;
- ISO No. 27002 [supersedes ISO No. 17799], “Information technology - Security techniques - Code of practice for information security management” of the International Organization for Standardization;
- Statement on Standards for Attestation Engagements No. 16 (SSAE 16) for reporting on controls at service organizations [supersedes SAS 70 report]; and
- The Federal Risk and Authorization Management Program (FedRAMP) standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The standards that form the backbone of this document are primarily designed for the evaluation and accountability of general, application and security controls over financial information systems that support a business operation. In this case, the controls apply to the calculation by an automated system and/or service provider of the proper and correct sales and use taxes to be applied to sales made in each jurisdictional environment in which common administrative standards and definitions found in the SSUTA have been adopted and employed.

The core of the CSP/CAS systems will be interactive Internet-based transactions between the sellers and the CSP/CAS, and data transmissions between the CSP/CAS, States, and Governing Board. These standards reflect commonly accepted “best practices” for an interactive Internet environment, including the use of cloud-based systems.

This document uses a deductive, “drill-down” approach, and is laid out as follows:

SECTION I consists of this introductory narrative that explains, in general terms, the purpose and scope of the certification and audit standards adopted by the Member States.

SECTION II is a high-level summary of the standards to be used for evaluating, certifying and auditing the automated systems and providers as defined in the SSUTA.

SECTION III contains a detailed explanation of each of the standards to be used in the evaluation process.

## SECTION II - CERTIFICATION STANDARDS SUMMARY

### 100 ~ GENERAL CONTROLS

Must demonstrate that the appropriate *general controls* are in place (see Footnote 1)

- Security management
- Access controls
- Configuration management
- Segregation of duties
- Contingency planning

### 200 ~ BUSINESS PROCESS APPLICATION CONTROLS

Must demonstrate that the appropriate *business process application controls* are in place (see Footnote 1):

- Application level general controls
- Business process controls
- Interface controls
- Data management system controls

### 300 ~ ADMINISTRATION OF SOFTWARE AND DATABASES

Must demonstrate the accuracy of modifications to systems and databases by testing of the systems and software in coordination with Testing Central. Tests may be performed by the Member States as a group through remote access or onsite at the CSP, or by individual Member States through remote access only.

### 400 ~ SUFFICIENCY OF INFORMATION

Must consider the necessary mechanisms to be built into the system in order to:

- Demonstrate the system's ability to capture and retain sufficient information to

- make an accurate tax determination, and provide an accurate tax filing.
- Demonstrate the system's ability to obtain, accumulate and report information on exempt sales.
- Demonstrate the proper use of state-provided sourcing information and compliance with state laws pertaining to taxability of TPP and Services.

#### 500 ~ TRANSMISSION AND SECURITY OF DATA

Must process transactions at industry-standard speeds and provide adequate security over data, both internally and externally.

#### 600 ~ PRIVACY STANDARDS

Must meet privacy standards and properly protect data from misuse.

#### 700 ~ RIGHT TO CERTIFY, RECERTIFY, AND AUDIT

Must be able to provide information in electronic format as required for certification, recertification, and compliance audits. Must also agree to any generally accepted sampling procedures, including electronically applied statistical sampling. Systems must be structured to provide for this functionality.

Footnote 1: For those parts of systems or processes performed through a cloud vendor or other service provider, the Contractor must be able to obtain assurance that the appropriate controls and security requirements are in place. The ability to obtain this assurance should be documented in provider service agreements. Corroboration that these controls and security requirements are in place can be obtained through independent security audit reports (e.g., IT security audits, SSAE 16 reports). In cases where independent security audit reports are not available, written representations from provider management may be acceptable.

## SECTION III - DETAILED CERTIFICATION STANDARDS

### 100 ~ General Controls

Must demonstrate that the following *general controls* are in place, where appropriate:

#### 110 SECURITY MANAGEMENT

An entity wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Critical Elements for Security Management:

- A. Establish a security management program.
  - The security management program is adequately documented, approved, and up-to-date.
  - A security management structure has been established.
  - Information security responsibilities are clearly assigned.
  - Subordinate security plans are documented, approved, and kept up-to-date.
  - An inventory of systems is developed, documented, and kept up-to-date.
- B. Periodically assess and validate risks.
  - Risk assessments and supporting activities are systematically conducted.
- C. Document and implement security control policies and procedures.
  - Security control policies and procedures are documented, approved by management and implemented.
- D. Implement effective security awareness and other security-related personnel policies.
  - Owners, system administrators, and users are aware of security policies.
  - Hiring, transfer, termination, and performance policies address security.
  - Employees have adequate training and expertise.
- E. Monitor the effectiveness of the security program.
  - The effectiveness of security controls is periodically assessed.
- F. Effectively remediate information security weaknesses.
  - Information security weaknesses are effectively remediated.
- G. Ensure that activities performed by external third parties are adequately secure.

- External third party activities are secure, documented, and monitored.

SPECIFIC REQUIREMENT IN APPLYING FOR CERTIFICATION:

As a part of the initial certification, the *Streamlined Sales Tax Evaluation Committee Security Self-Assessment Questionnaire* must be completed. This document was adapted from the questionnaire that was included in the “Risk Management Guide for Information Technology Systems” that was created by the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce.

## 120 ACCESS CONTROLS

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or exfiltrate data or execute changes that are outside their span of authority.

### Critical Elements for Access Control:

- A. Adequately protect information system boundaries.
  - Appropriately control connectivity to system resources.
  - Appropriately control network sessions.
- B. Implement effective identification and authentication mechanisms.
  - Users are appropriately identified and authenticated.
- C. Implement effective authorization controls.
  - User accounts are appropriately controlled.
  - Processes and services are adequately controlled.
- D. Adequately protect sensitive system resources.
  - Access to sensitive system resources is restricted and monitored.
  - Adequate media controls have been implemented.
  - Cryptographic controls are effectively used.

- E. Implement an effective audit and monitoring capability.
  - An effective incident response program is documented and approved.
  - Incidents are effectively identified and logged.
  - Incidents are properly analyzed and appropriate actions taken.
  
- F. Establish adequate physical security controls.
  - Establish a physical security management program based on risk.
  - Establish adequate perimeter security based on risk.
  - Establish adequate security at entrances and exits based on risk.
  - Establish adequate interior security based on risk.
  - Adequately protect against emerging threats based on risk.

SPECIFIC SECURITY REQUIREMENT:

Interactive transactions should only be accepted from authorized users.

1. Sellers sending sales transactions through the CSP/CAS should first authenticate themselves to the system. Each transaction should include identification unique to the seller; the ideal is for each transaction to be digitally signed.
  
2. For remote access, either by sellers or for audit or certification processes, secure access such as a Virtual Private Network (VPN) should be utilized.

## 130 CONFIGURATION MANAGEMENT

Configuration management (CM) involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

Critical Elements for Configuration Management:

- A. Develop and document CM policies, plans, and procedures.
  - CM policies, plans, and procedures have been developed, documented, and implemented.
  
- B. Maintain current configuration identification information.
  - Current configuration identification information is maintained.
  
- C. Properly authorize, test, approve, and track all configuration changes.
  - All configuration changes are properly managed (authorized, tested, approved, and tracked).

- D. Routinely monitor the configuration.
  - The configuration is routinely audited and verified.
- E. Update software on a timely basis to protect against known vulnerabilities.
  - Software is promptly updated to protect against known vulnerabilities.
- F. Appropriately document and approve emergency changes to the configuration.
  - Adequate procedures for emergency changes are documented and implemented.
  - Emergency changes to the configuration are documented and approved.

## 140 SEGREGATION OF DUTIES

Effective segregation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. Work responsibilities should be segregated so that one individual does not control all critical stages of a process. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Inadequately segregated duties, conversely, increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

Critical Elements for Segregation of Duties:

- A. Segregate incompatible duties and establish related policies.
  - Incompatible duties have been identified and policies implemented to segregate these duties.
  - Job descriptions have been documented.
  - Employees understand their duties and responsibilities.
- B. Control personnel activities through formal operating procedures, supervision, and review.
  - Formal procedures guide personnel in performing their duties.
  - Active supervision and review are provided for all personnel.

## 150 CONTINGENCY PLANNING

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.



It is critical that an entity have in place (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions, and (2) a plan to recover critical operations should interruptions occur.

Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions.

**Critical Elements for Contingency Planning:**

- A. Assess the criticality and sensitivity of computerized operations and identify supporting resources.
  - Critical data and operations are identified and prioritized.
  - Resources supporting critical operations are identified and analyzed.
  - Emergency processing priorities are established.
  
- B. Take steps to prevent and minimize potential damage and interruption.
  - Information system backup and recovery procedures have been implemented.
  - Adequate environmental controls have been implemented.
  - Staff have been trained to respond to emergencies.
  - Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.
  
- C. Develop and document a comprehensive contingency plan.
  - An up-to-date contingency plan is documented.
  - Arrangements have been made for alternate data processing, storage, and telecommunications facilities.
  
- D. Periodically test the contingency plan and adjust it as appropriate.
  - The plan is periodically tested.
  - Test results are analyzed and the contingency plan is adjusted accordingly.

**200 ~ Application Controls**

Must demonstrate that the following *business process application controls* are in place, where appropriate:

**210 APPLICATION LEVEL GENERAL CONTROLS**

Application level general controls (referred to herein as “application security” or AS) consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.

The critical elements for application level general controls are:

- A. Implement effective application security management.

- A comprehensive application security plan is in place.
- Application security risk assessments and supporting activities are periodically performed.
- Policies and procedures are established to control and periodically assess the application.
- Application owners and users are aware of application security policies.
- Management monitors and periodically assesses the appropriateness of application security policies and procedures, and compliance with them.
- Management effectively remediates information security weaknesses.
- External third party provider activities are secure, documented, and monitored.

B. Implement effective application access controls.

- Application boundaries are adequately protected.
- Application users are appropriately identified and authenticated.
- Security policies and procedures appropriately address ID and password management.
- Access to the application is restricted to authorized users.
- Public access is controlled.
- User access to sensitive transactions or activities is appropriately controlled.
- Sensitive application resources are adequately protected.
- An effective access audit and monitoring program is in place, documented, and approved.
- Application security violations are identified in a timely manner.
- Exceptions and violations are properly analyzed and appropriate actions are taken.
- Physical security controls over application resources are adequate.

C. Implement effective application configuration management.

- Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly.
- Current configuration information is maintained.
- A system development life cycle methodology has been implemented.
- Authorizations for changes are documented and maintained.
- Changes are controlled as programs progress through testing to final approval.
- Access to program libraries is restricted.
- Movement of programs and data among libraries is controlled.
- Access to application activities/transactions is controlled via user roles (access privileges).
- Access to all application programs/codes and tables are controlled.
- Access to administration (system) transactions that provide access to table maintenance and program execution is limited to key users.
- Access and changes to programs and data are monitored.

- Changes are assessed periodically.
  - Applications are updated on a timely manner to protect against known vulnerabilities.
  - Emergency application changes are properly documented, tested, and approved.
- D. Segregate application user access to conflicting transactions and activities and monitor segregation.
- Incompatible activities and transactions are identified.
  - Application controls prevent users from performing incompatible duties.
  - There is effective segregation of duties between the security administration function of the application and the user functions.
  - User access to transactions or activities that have segregation of duties conflicts is appropriately controlled.
  - Effective monitoring controls are in place to mitigate segregation of duty risks.
- E. Implement effective application contingency planning.
- Assess the criticality and sensitivity of the application through a Business Impact Analysis (BIA) or equivalent.
  - Take steps to prevent and minimize potential damage and interruption.
  - Develop and document an application Contingency Plan.
  - Periodically test the application contingency plan and adjust it as appropriate.

**SPECIFIC CONTINGENCY PLANNING REQUIREMENT:**

Store-and-forward capability as backup to real-time mode. Transmission channels, including the Internet, are not always available. Interactive systems between sellers and the CSP/CAS should be developed so that if the communications are interrupted, transactions are stored in a temporary file, and then forwarded automatically to the receiving system when communications are restored. Transactions logs and control records should be able to verify that all transactions have been forwarded and that the system is “made whole” as if the interruption to communications had not happened.

## 220 BUSINESS PROCESS CONTROLS

Business Process (BP) controls are the automated and/or manual controls applied to business transaction flows. They relate to the completeness, accuracy, validity and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

The critical elements for business process controls are:

- A. Transaction Data Input is complete, accurate, valid, and confidential (transaction data input controls).
- A transaction data strategy is properly defined, documented, and appropriate.
  - Source documentation and input file data collection and input preparation and entry is effectively controlled.
  - Access to data input is adequately controlled.
  - Input data are approved.
  - Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing.
  - Input values to data fields that do not fall within the tolerances or parameters determined by the management result in an automated input warning or error.
  - Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.
  - Errors are investigated and resubmitted for processing promptly and accurately.
- B. Transaction Data Processing is complete, accurate, valid, and confidential (transaction data processing controls).
- Application functionality is designed to process input data, with minimal manual intervention.
  - Processing errors are identified, logged and resolved.
  - Transactions are executed in accordance with the predetermined parameters and tolerances, specific to entity's risk management.
  - Transactions are valid and are unique (not duplicated).
  - The transactions appropriately authorized.
  - Data from subsidiary ledgers are in balance with the general ledger.
  - User-defined processing is adequately controlled.
  - As appropriate, the confidentiality of transaction data during processing is adequately controlled.
  - An adequate audit and monitoring capability is implemented.
- C. Transaction Data Output is complete, accurate, valid, and confidential (transaction data output controls).
- Outputs are appropriately defined by the management (form, sensitivity of data, user selectivity, confidentiality, etc.).
  - Output generation and distribution are aligned with the reporting strategy.
  - System generated outputs/reports are reviewed to reasonably assure the integrity of production data and transaction processing.
  - Output/reports are in compliance with applicable laws and regulations.
  - Access to output/reports and output files is based on business need and is limited to authorized users.
- D. Master Data Setup and Maintenance is adequately controlled.
- Master data are appropriately designed.
  - Changes to master data configuration are appropriately controlled.
  - Only valid master records exist.

- Master data are complete and valid.
- Master data are consistent among modules.
- Master data additions, deletions, and changes are properly managed and monitored by data owners.
- As appropriate, the confidentiality of master data is adequately controlled.

#### SPECIFIC SECURITY REQUIREMENTS:

1. In the Internet environment, transactions from sellers to the CSP/CAS may be formatted using eXtensible Markup Language (XML). The use of predefined XML schemas, against which the transactions are validated, can provide edit checks as the data enters the system. XML schema standards for transactions between the CSP/CAS and state agencies ~~are being defined, and will~~ allow states to validate the incoming data at point of entry.
2. Overriding or bypassing data validation and editing is restricted. Many systems allow data validation and edit routines to be bypassed, which could allow the system to accept and process erroneous data. Using the bypass capability (sometimes referred to as an override) should be very limited and closely controlled and monitored by supervisory personnel. For example, each override should be automatically logged and reviewed by supervisors for appropriateness and correctness.

### 230 INTERFACE CONTROLS

Interface controls (IN) consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion.

The critical elements for interface controls are:

- A. Implement an effective interface strategy and design.
  - An interface strategy is developed for each interface used in the application.
  - An interface design is developed for each interface used in the application that includes appropriate detailed specifications.
- B. Implement effective interface processing procedures.
  - Procedures are in place to reasonably assure that the interfaces are processed accurately, completely and timely.
  - Ownership for interface processing is appropriately assigned.

- The interfaced data is reconciled between the source and target application to ensure that the data transfer is complete and accurate.
- Errors during interface processing are identified by balancing processes and promptly investigated, corrected and resubmitted for processing.
- Rejected interface data is isolated, analyzed and corrected in a timely manner.
- Data files are not processed more than once.

## 240 DATA MANAGEMENT SYSTEM CONTROLS

Data management system (DA) controls are relevant to most business process applications because applications frequently utilize the features of a data management system to enter, store, retrieve or process information, including detailed, sensitive information such as financial transactions, customer names, and social security numbers.

The critical elements for data management controls include:

- A. Implement an effective data management system strategy and design.
  - Implement an effective data management system strategy and design, consistent with the control requirements of the application and data.
  - Detective controls are implemented in a manner that effectively supports requirements to identify and react to specific system or user activity within the data management system and its related components.
  - Control of specialized data management processes used to facilitate interoperability between applications and/or functions not integrated into the applications (such as ad-hoc reporting) are consistent with control requirements for the application, data and other systems that may be affected.

## ***300 ~ Administration of Software and Databases***

### *Requirements:*

Must demonstrate the accuracy of modifications to systems and databases by tests of the systems and software. Tests may be performed by the Member States as a group through remote access or onsite at the CSP, or by Individual States through remote access only.

### *General Discussion:*

Software systems and the databases that support them are only as good as the data is accurate. It is essential to not only test the software to ensure it functions correctly, but to have appropriate change controls in place over program and database modifications to ensure continuing accuracy.

### *The Controls:*

## 310 ADMINISTRATION OF SOFTWARE MODIFICATIONS

Only authorized software modifications should be made to the application system. Modifications should only be released after thorough testing.

- A. All software modifications are tested by personnel independent of the programming function. The following type of testing should occur:
1. Regression Testing. Regression testing focuses on the following:
    - Do the unmodified functions still operate as expected after a change has been introduced?
    - Does everything work together as before after all changes and fixes have been introduced?
  2. Interface Testing. Testing of the interfaces to other existing internal or external systems and databases should be repeated after modifications are made to ensure nothing got broke in the process.
  3. End-to-end Functionality Testing. The entire transaction cycle must be re-tested after any software modifications to ensure that everything is functioning correctly.
- B. All databases are inspected for accurate data after programming modifications are made. The integrity of application data can be compromised by software modifications that produce unintended results. Examples include:
1. Inspection of data elements. To counter the risk of introducing inaccurate data into databases after programming modifications are made, all data elements should be examined for correctness.

2. Testing databases for referential integrity. Data should be correct when taken as a whole and not have missing elements. For example, if a taxpayer registration number is designated as the primary key for a table, then each row in the table must have a taxpayer registration number attribute. If a sale transaction is classified as exempt, all data elements should be present. If missing data elements exist, the CSP should have processes in place to detect and obtain the missing data elements.
  3. Testing databases for entity integrity. For example, if a transaction number is a mandatory field, then an attribute of Null is not allowed. Otherwise the entity integrity has been violated.
- C. Updates to the taxability matrix as approved by the Governing Board shall be adequately documented.

Section 328 of the Streamlined Sales and Use Tax Agreement requires each Member State to provide notice of changes in the taxability of products or services listed in the taxability matrix.

1. Changes to the taxability matrix shall be completed on a quarterly basis with proper documentation maintained for all changes.
2. Sellers and CSPs are relieved from liability to a Member State or its local jurisdiction if incorrect information was provided by the Member State. However, failure of a Member State to provide notice of a rate change shall not relieve the seller from its obligation to collect sales and use taxes for that Member State. (See sections 304, 305 & 328 of the SSUTA.)
3. Rate changes shall be properly implemented and documented by the CSP and CAS.

## 320 ADMINISTRATION OF CHANGE CONTROLS

All versions of software must be tracked with some kind of change control process, to ensure that the appropriate level of software modification is matched to the data processed.

- A. Version Control. All software modules must be kept under the operation of a Version Control system.
- B. No Unauthorized Modifications. Only programming changes that have been tested and approved by management to be migrated to production should be allowed.



- C. Separate Programming Libraries should be maintained. Data libraries will be separated by test or production data.
- D. All changes and overrides must be properly documented.

### 330 DATA REDUNDANCY AND REPAIRABILITY

Data should be protected against corruption or loss due to hardware failure through implementations that provide data redundancy and repairability.

- A. Hardware implementations for critical data should allow the data to be recovered automatically in the event of corruption or loss due to hardware failure. Techniques such as the use of RAID storage, database server clustering and mirroring should be utilized as appropriate and cost effective.
- B. Backups of production data must be taken at regular intervals. Transaction logs should be utilized so that if a database failure occurs, the combination of backup files and transaction logs can be utilized to recover the data up to the exact point of failure.

### ***400 ~ Sufficiency of Information***

Must consider the necessary mechanisms to be built into the system in order to:

- A. Demonstrate the system's ability to capture and retain sufficient information to make an accurate tax determination, and provide an accurate tax filing.

Build into the system the appropriate features for providing assurance that adequate information is obtained from the purchaser, the seller, and the applicable state(s) so that the correct amount of tax is calculated, collected, reported and remitted. This requires among other features:

- Timely updates of state taxability matrices from the individual states.
- Providing evidence of the transmission of the tax to the applicable state.
- Providing evidence that the matrix update has been received, is complete, and tested. Providing evidence that the matrix update has been loaded to the system according to appropriate software library procedures, and is logged as being loaded.
- The history of product code mapping to the taxability matrix is available on-line, or in archive form that is retrievable and restorable in the format and time period designated by the Governing Board and Member States.
- Audit trails that evidence each of the above.

- B. Demonstrate the system's ability to obtain, accumulate and report information on

exempt sales.

- Build into the system the appropriate features for providing assurance in cases of exempt sales that adequate information is obtained from the purchaser, the seller, and the applicable state(s). This requires:
- The system must accumulate exempted sales by purchasing entity and be able to provide this information in aggregate or detail, as required by Appendix F of the Governing Board Rules
- Audit trails that evidence the above.

C. Demonstrate the proper use of member states sourcing rules and state-provided matrixes and compliance with state laws pertaining to taxability of TPP, digital equivalents and services.

Build into the system the appropriate features for testing the matrix updates from the individual states, as well as providing internal tests of compliance with the individual state laws pertaining to taxability of TPP and Services. This requires:

- Sufficient tests of matrix updates to assure they work correctly, per Appendix E of the Governing Board Rules.
- The CSP shall have sufficiently trained staff responsible for administering the operating systems which compute the correct amount of tax and remittance in accordance with the specific requirements of the individual states.
- Appropriate quality review programs and internal audits to provide quality assessments and oversight over the systems and processing.
- Sourcing – A standard format for tax jurisdiction codes shall be employed to match physical street addresses to the proper taxing jurisdiction. Unless otherwise authorized by the Governing Board, CAS, CSP and state revenue departments shall all use the coding format authorized in Section 119 of the Mobile Telecommunications Sourcing Act (P.L. 106-252) and approved by the Multistate Tax Commission (MTC) and the federation of Tax Administrators (FTA).
- Audit trails that evidence each of the above.

D. Sales Tax Holidays (Complete after final determination)

E. Bundling Requirements (Complete after SST final determination)

F. All records that relate to transactions handled through Certified Automated Systems (CAS) and Certified Service Providers (CSP) shall be maintained in electronically accessible form for no less than four (4) years from the due date of the relevant filing period, or the date of actual filing, whichever occurs later.

## **500 ~ Data Transmission Security Standards**

### *Introduction:*

A critical element in the certification process is the assurance that data exchanged between all parties is secure, non-repudiated, and unaltered. To that end, the SST requires that all certified service providers and all certified automated systems adhere to the following provisions, in addition to those contained in the Streamlined Sales Tax Implementation Guide:

### **510 ENCRYPTION**

All transmissions will be encrypted and will require the use of a digital certificate containing a key no less than 128 bits in length.

### **520 TRANSMISSIONS BETWEEN CSP/CAS, MEMBER STATES, AND THE GOVERNING BOARD.**

The Governing Board and each Member State will each prescribe the method for transmission of tax returns and other required reporting. Permissible transmission methodologies include:

- A. Secure upload and download by means of HTTPS protocol utilizing Secure Sockets Layer (SSL) encryption. States will provide a secure HTTPS site based on a certificate containing a key no less than 128 bit in length.
- B. Secure application-to-application web services, also utilizing HTTPS.
- C. Secure FTP upload and download. States will provide a secure FTP server, or require commercially available strong encryption software such as PGP ("Pretty Good Privacy"). Zip compression/encryption is considered weak encryption and will not be acceptable.

### **530 TRANSMISSIONS BETWEEN SELLERS AND THE CSP/CAS.**

CSPs and users of CAS systems will prescribe the methodology for transmission of transactions between sellers and the CSP/CAS. All such transactions must be encrypted, and the CSP/CAS implementation must provide a certificate containing a key no less than 128 bytes in length. It is anticipated that all Internet transactions between sellers and the CSP/CAS will utilize HTTPS with SSL.

### **540 DIGITAL SIGNATURES**

When a message is received, the recipient may desire to verify that the message has not

been altered in transit. Furthermore, the recipient may wish to be certain of the originator's identity. Both can be accommodated by the Digital Signature Algorithm (DSA). A digital signature is an electronic analog of a written signature in that the digital signature can be used in proving to the recipient, or a third party, that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time.

This document stops short of requiring the use of digital signatures for all transmissions, due to the difficulties in interoperability among certificate authorities, as well as the processing overhead involved, and the expense and complexity that would be required for the smaller sellers. Because of these considerations, few states have implemented digital signature processes with their electronic partners. However, the use of digital signatures remains the "gold standard" of authentication, non-repudiation, security, and integrity, and should be implemented when the technology becomes practical.

For further information concerning digital signatures, this document refers the reader to:

- FIPS 46-2 – Digital Encryption Standard
- FIPS 186 – Digital Signature Standard

This publication prescribes the Digital Signature Algorithm (DSA) for digital signature generation and verification. In addition, the criteria for the public and private keys required by the algorithm are provided.

Additional FIPS standards that pertain to data encryption under this certification standard:

- FIPS 140-1 – Security Standards for Cryptographic Modules
- FIPS 171 – Key management Using ANSI X9.17
- FIPS 180-1 – Digital Hash Standard
- FIPS 185 Escrowed Encryption Standard
- FIPS 196 Public Key Cryptographic Entity Authentication Mechanism

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949, as amended by the Computer Security Act of 1987, Public Law 100-235.

Equivalent standards concerning digital signatures are contained in:

- ANSI X5.09 – Digital Certificates
- ANSI X9.30 – Public key Cryptographic Using Irreversible Algorithms
- ANSI X9.42 – Symmetric Algorithms Using Diffie-Hellman
- ANSI X9.55 – Extension to Public Key Certificates and Certificate Renovation List
- ANSI X9.23 – Message Confidentiality
- ANSI X9.9 – Message Authentication Codes

- ANSI X9.45 – Management Controls
- ANSI X9.17 – Financial Institution Key Management

The American National Standards Institute (ANSI) is a private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The organization's Headquarters are located in Washington, D.C., but an office in New York City is ANSI's operations center and the point of contact for all press inquiries. Most of the ANSI standards are functionally equivalent to the FIPS standards issued through the National Institute of Standards and Technology (NIST).

## 550 TRANSMISSION STORAGE AND PROTECTION

It is expected that CSPs will receive sales ~~retail~~ transactions continuously from online sellers over the Internet. In this and similar settings, the following apply:

- A. 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.
- B. 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.
- C. Transaction data should 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.
- D. CSPs shall install and maintain intrusion detection software to monitor their networks for any unauthorized attempt to access tax data.
- E. A CSP employing a cloud-based system or using a service provider for similar functions related to transmission storage and protection shall include these specific requirements in its provider service agreement. It should also obtain assurances from the provider that these contract requirements have been complied with.

## 560 VIRUS PROTECTION

CSPs and users of CAS systems shall install and maintain commercially accepted virus protection software and stay current with updates to that software. CSPs and users of CAS systems shall take all reasonable precautions to ensure that files sent to states are not contaminated by viruses.

## **600 ~ Privacy Standards**

Confidentiality and Privacy Protections for Model 1 taxpayers who use a Certified Service Provider are addressed in Section 321 of the Streamlined Sales and Use Tax Agreement. As stated in the SSUTA the Confidentiality and Privacy Protections are the protection of confidentiality rights of all participants in the system and of the privacy interests of consumers who deal with Model 1 sellers.

### **610 CONFIDENTIAL TAXPAYER INFORMATION**

- A. The SSUTA defines “confidential taxpayer information” as all information that is protected under a Member State’s laws, regulations, and privileges: the term “personally identifiable information” means information that identifies a person; and the term “anonymous data” means information that does not identify a person.
- B. A fundamental precept in Model 1 is to preserve the privacy of consumers by protecting their anonymity. With very limited exceptions, a Certified Service Provider (CSP) shall perform its tax calculation, remittance, and reporting functions without retaining the personally identifiable information of consumers.
- C. Other than as provided in section 620(D), confidential and proprietary information will not be sold or re-used in any way, even if the identity of the businesses using the solution can be masked.

### **620 PERSONALLY IDENTIFIABLE INFORMATION**

The CSP’s system must be designed and tested to ensure that the fundamental precept of anonymity is respected.

- A. Personally identifiable information is only used and retained to the extent necessary for the administration of Model 1 with respect to exempt purchasers. Street-level addresses, though, are required to be retained for all transactions for verifying that the correct jurisdictions were used.
- B. The CSP provides consumers clear and conspicuous notice of its information practices, including what information it collects, how it collects the information, how it uses the information, how long if at all, it retains the information and whether it discloses the information to Member States. Such notice shall be satisfied by a written privacy policy statement accessible by the public on the official web site of the CSP.
- C. The CSP’s collection, use and retention of personally identifiable information will be limited to that required by the Member States to ensure the validity of exemptions

from taxation that are claimed by reason of a consumer's status or the intended use of the good or services purchased.

- D. The CSP will provide adequate technical, physical, and administrative safeguards, including appropriate access controls, so as to protect personally identifiable information from unauthorized access and disclosure.

## 630 STATE REQUIREMENTS

- A. Each Member State shall provide public notification to consumers, including their exempt purchasers, of the state's practices relating to the collection, use and retention of personally identifiable information.
- B. When any personally identifiable information that has been collected and retained is no longer required for the purposes set forth, above, such information shall no longer be retained by the Member States.
- C. When personally identifiable information regarding an individual is retained by or on behalf of a Member State, such state shall provide reasonable access by such individual to his or her own information in the state's possession and a right to correct any inaccurately recorded information.
- D. If anyone other than a Member State, or a person authorized by the state's law or the SSUTA, seeks to discover personally identifiable information, the state from whom the information is sought should make a reasonable and timely effort to notify the individual of such request.
- E. This privacy policy is subject to enforcement by Member States' attorneys general or other appropriate state government authority.
- F. Each Member States' laws and regulations regarding the collection, use, and maintenance of confidential taxpayer information remain fully applicable and binding. Without limitation, the SSUTA does not enlarge or limit the Member States' authority to:
  1. Conduct audits or other review as provided under the SSUTA and state law.
  2. Provide records pursuant to a Member States' Freedom of Information Act, disclosure laws with governmental agencies, or other regulations.
  3. Prevent, consistent with state law, disclosures of confidential taxpayer information.
  4. Prevent, consistent with federal law, disclosures or misuse of federal return information obtained under a disclosure agreement with the Internal Revenue Service.
  5. Collect, disclose, disseminate, or otherwise use anonymous data for governmental purposes.

- G. This privacy policy does not preclude the Governing Board from certifying a CSP whose privacy policy is more protective of confidential taxpayer information or personally identifiable information than is required by the SSUTA.

### **700 ~ Right To Certify, ~~or~~ Recertify, and Audit**

Under Models 1 and 2, Certified Service Providers and Certified Automated System Providers (CAS) are required to provide the auditors with sufficient and timely access to those systems that the auditors deem necessary for performing the certification or recertification of the CSP and the CAS.

The auditors are to be provided with access to any documentation, system, and database or system component, needed for them to perform the certification or re-certification.

The CSP and CAS Providers will provide auditors with access to all appropriate staff, including, but not limited to, systems, security, disclosure, legal and accounting.

The CSP and CAS Providers shall allow for the performance of an evaluation for certification and recertification by the SST Governing Board Certification Committee ~~Member States~~ or any agent or representative designated by the SST Governing Board ~~Member States~~.

The CSP and CAS Providers will allow for contract compliance audits to be conducted by the Audit Core Team of the SST Audit Committee, as well as multi-jurisdictional tax audits to be conducted by the Member States or any agent or representative designated by the SST Governing Board Member States.

The CSP and CAS Providers shall allow for the use of any generally accepted auditing procedures, unless it is agreed that other valid testing procedures are more appropriate. {The auditors will conduct their audits in conformance with audit standards approved by the Governing Board. The CSP and CAS Providers should not be in a position to control the “standards” used by the auditors. On the other hand, there may be instances that may limit the procedures that can be performed. For example, performing electronic tests on an active computer system could cause serious system overhead that could reduce response time, or even bring down the system.}

The CSP and CAS Providers shall agree to provide electronic records for the certification, ~~or~~ recertification, and audit process on a timely basis, as set forth in Appendix E (Testing Process for Certification of Service Providers and Automated Systems) and Appendix F (SST Reports) of the SST Governing Board Rules. Appendix F describes the format in which electronic records will be provided, as well as establishes the requirements for the administration site to be provided by each CSP and CAS Provider. The CSP and CAS Provider shall provide all necessary fields within each record and an accompanying data dictionary that explains the characteristics of each field.

The CAS or CSP shall agree to use generally accepted sampling procedures. Statistical



sampling will be the default sampling procedure unless it is agreed other valid sampling procedures are more appropriate.