A motion by Kentucky on behalf of the Certification Committee to amend Appendix C (Sections E.6, I.5 and I.6) to make it consistent with Appendix G

Appendix C (Summary Showing Sections Changed – Changes Highlighted in Green)

The following changes were made in Appendix C. References were added to the corresponding Section in Appendix G.

E. 6	Applicant has a policy utilizing industry-standard availability/fault tolerance benchmarks. **{see Section 160 of the Certification Standards (Appendix G)}**	Plan to describe the redundancy, fail over capability, and availability of the system.

I. 5	A cyber security policy is in place. **{see Sections 570 of the Certification Standards (Appendix G)}**	Copy of policy describing processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Should include actions to be taken in response to security incidents.
6	A telecommuting policy is in place. **{see Sections 570 of the Certification Standards (Appendix G)}**	Copy of telecommuting policy for employees and subcontractors. Should include written telecommuting agreement, telecommuting safety checklist, and approval of mobile technology.

Full Document with Changes Tracked

Appendix C (8-18-2020)

	Criteria for CSP Evaluation	**Additional Information/Explanation**
	Any changes in partners, subcontractors, key personnel, financial condition or other material information on this application, must be submitted via an addendum with the same detail as required on the original application. Addendums will require additional evaluation and must be approved by the Governing Board.	
A	**Corporate Background and Experience:** **(Attach documentation to the application for all items requested in Section A)**	
1	Include background information of the applicant along with detailed experience with similar projects or other information that demonstrates that the applicant is qualified.	Must have similar: 1. Project tax experience, 2. Size and complexity, or 3. Project implementation.
2	If similar work has been performed for others, list three references (with contact names and telephone numbers) for whom such work was performed.	

3	If applicable, list subcontractors and/or partners that the applicant intends to use in fulfilling any contract entered into. Attach to this list a description of the work that will be subcontracted or performed by the partner and an explanation of the capabilities of the subcontractor/partner, including the history and relationship to the applicant.	A list of all subcontractors and/or partners must be submitted to and approved by the Governing Board and may require additional evaluation.
4	If this application is on behalf of a partnership or other multi-party entity, identify each entity and provide background and experience information for each.	
5	Specify and provide information on any key personnel employed by the applicant, subcontractors, or partners. This includes the experience of these key persons and a brief summary of the type of work they will perform.	
6	Provide a statement of criminal history acknowledging whether the applicant, or any of its subcontractors or partners, including their officers, directors, or key personnel, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriations or deception. If there is no existence of criminal history, an acknowledgement to that effect must be provided.	Background checks may be required.
7	Provide a statement indicating that for purposes of any work performed under this contract, the applicant, along with its partners and subcontractors, will maintain their books, records, computer systems, data, and backup facilities in the United States.	
B	**Financial Soundness:** **(Attach documentation to the application for all items requested in Section B)**	
1	A business plan encompassing the CSP operations, signed by the applicant. If the business plan includes a subcontractor or partnership, the business plan includes details of the specific functions to be performed by each party.	Business plan should encompass three years of operations, including the start-up period and the first two years of operations. This should include separate cost components detailing system development costs, staffing costs, equipment and other fixed asset needs, facilities, and other necessary administrative and operating costs covering the start-up and contract periods. Financing sources should be sufficient to demonstrate the viability of the applicant's business plan.

2	Audited financial statements for the last 3 years with a current certification from the chief financial officer stating that the statements are current, accurate and complete. Exceptions regarding any materially adverse changes since the date of the most recent financial statements were disclosed, if applicable.	The financial statements must include the basic financial statements and notes to financial statements as defined by generally accepted accounting principles, as well as an auditor's opinion. If no audited financial statements are available, unaudited financial statements with a current certification from the chief financial officer or similar officer would be sufficient. If the company has been in business for less than 3 years, provide the financial statements for the period it has been in existence.
3	If the applicant is a subsidiary of another corporation, submit unaudited financial statements with a certification from the CFO that statements were used to prepare audited parent company financial statements, in addition to submitting the audited financial statements of the parent company.	Financial statements must provide a clear picture of the financial health of the subcontractors and partners.
4	The following standard "Financial Ratios" for the last 3 years: Current Ratio; Quick Ratio; Net Working Capital Ratio; Profit Margin Ratio; Accounts Receivable Turnover Ratio & Debt to Equity Ratio.	Ratios must be within recognized industry norms.
5	If the applicant is a subsidiary, provide the "Financial Ratios" stated above for consolidated financial statements of the parent company.	Ratios must be within recognized industry norms.
6	If this application is submitted on behalf of a partnership or other multi-party entity, include the financial information listed above for each of the parties.	
C	**Project Staffing and Organization** **(Attach documentation to the application for all items requested in Section C, including an Organization Chart)**	
1	The name, address, and telephone number of a person with authority to bind the applicant.	
2	The name, address, and telephone number of a person who can answer questions or provide clarification concerning this application.	
3	Provide details of the proposed staffing and deployment of personnel to be assigned to the contractual undertaking should a contract be entered into (including information about the qualifications and experience of all key personnel).	
D	**Technical Approach** **(Applicant's system must comply with all requirements listed in Section D. Attach documentation to the application for all items requested in Section D.)**	

1	Applicant's system complies with the Uniform Sourcing requirement and accommodates sourcing rules of Associate Member States **{see Section 309 of the Streamlined Agreement, Section 400 (C) of the Certification Standards (Appendix G)}**	This is verified through the results from the system test process.
2	Applicant's system complies with the Exemption Processing requirement **{see Section 317 of the Streamlined Agreement, Section 620 (D) of the Certification Standards (Appendix G)}**	This is verified through the results from the system test process.
3	Applicant's system response complies with the Uniform Rounding requirement **{see Section 324 of the Streamlined Agreement}**	This is verified through the results from the system test process.
4	Applicant's system complies with the Uniform Definitions requirement **{see Section 104 and Appendix C of the Streamlined Agreement}**	This is verified through the results from the system test process.
5	Applicant's system complies with the Rate and Boundary Changes requirement **{see Section 305 of the Streamlined Agreement}**	This is verified through the results from the system test process.
6	Applicant's system complies with the Tax Collection Procedures requirement **{see Section 319 of the Streamlined Agreement}**	This is verified through the results from the system test process.
7	Applicant's system complies with the Liability Relief requirement **{see Section 306 of the Streamlined Agreement}**	Must meet the requirement covered in Section 306 of the SSUTA.
8	Applicant's system complies with the Tax Remittance Procedures requirement **{see Section 319 of the Streamlined Agreement and Section 400 of the Certification Standards (Appendix G)}**	This is verified through the results from the system test process.
9	Applicant's system complies with the Tax Reporting Procedures requirement **{see Section 321 of the Streamlined Agreement and Section 520 of the Certification Standards (Appendix G)}**	This is verified through the results from the system test process.
10	Applicant's system complies with the Record Retention Procedures requirement **{see Section 630 of the Certification Standards (Appendix G) and Section 321 of the Streamlined Agreement}**	Records need to be maintained for a minimum of 4 years, and preferably 7 years.

11	Applicant's system complies with the Audit Requirements. Each applicant must demonstrate that it can provide information in electronic format as required for certification and audit; must agree to any generally accepted sampling procedures, including electronically applied statistical sampling; and must be able to demonstrate that its systems are structured to provide for this functionality. **{see Section 301 and 806(C) of the Streamlined Agreement, Sections 600 and 700 of the Certification Standards (Appendix G)}**	
12	Applicant's system complies with the Taxpayer Privacy requirement **{see Section 321 of the Streamlined Agreement and Section 600 of the Certification Standards (Appendix G)}**	Provide policy statements for each action they have invoked to meet the privacy standards and protection of data.
13	Applicant's application addressed the requirement for on-going real-time testing of the system including a method of conducting a performance test with an explanation of what will be revealed when the test is conducted (and the testing has confirmed this) **{see Section 300 of the Certification Standards (Appendix G)}**	Remote access testing should be available on an on-going basis; however, state submission of quarterly test files to CSPs will be coordinated through the Governing Board and the CSP testing contact.
14	Applicant's system has the capability and applicant assures that all taxes due will be collected and remitted to the appropriate Member states if the system is unavailable for a period of time.	Provide copy of disaster recovery plan. Describe the redundancy and fail over capability of the system to ensure there is no loss of taxes due.
15	Applicant's system has the capability to support applicant's statement of the lead time and information required to act on behalf of additional sellers in the event that a different CSP ceases operations for any reason.	Applicant stipulates how much lead time that it needs to act on behalf of additional sellers.
16	Applicant's system is able to generate, transmit, and receive a bulk registration to and from the SST Central Registration system. Transmission must be accomplished using web services and in the format approved by TIGERS and the SST Governing Board.	This is verified through the results from the system test process.
E	**Certification Standards - General Controls** **(Attach documentation to the application for all items requested in Section E)**	

1	Applicant has in place an entity-wide security management program that establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. **{see Section 110 of the Certification Standards (Appendix G)}**	Documents should include a detailed security management program that is adequately documented, approved, and up-to-date. The program should provide for an ongoing process of assessing risk, developing and implementing effective security procedures, monitoring the effectiveness of these procedures, and effectively remediating information security weaknesses. The application should also address security management related to those parts of the system related to the contract that are performed by subcontractors to provide assurance that external third-party activities are secure, documented, and monitored.
2	Applicant has access controls in place that limit and detect inappropriate access to computer resources (data, equipment, and facilities). The access controls should include both logical and physical controls. **{see Section 120 of the Certification Standards (Appendix G)}**	Access control policy should cover all points of access to the system and data, including base of operations, hosting site, and data backup installation. Since each of these systems may be owned by different parties, an understanding of the access control policies of each system should be obtained. Minimum standards for establishing physical and logical access controls include FISCAM AC 3.2 and NIST AC-1 through AC-22. Logical access controls should include authentication of users (e.g., passwords, other identifiers) that limit the files and other resources that can be accessed and the actions that can be executed. Physical access controls should restrict physical access to computer resources and data, as well as protect it from intentional or unintentional loss or impairment (e.g., persons gaining entry by going over the top of a partition, cutting a hole in a plasterboard wall). Documents should include a description of the access control policy that protects the Contractor's systems from unauthorized modification, loss, and disclosure. Logical access controls should provide authentication of users (e.g., passwords, other identifiers). Physical access controls (e.g., security at entrances and exits based on risk) should restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. An incident response program should also be included.
3	Applicant has in place a configuration management policy for the identification and management of security features for all hardware, software, and firmware components of the system. The configuration management system should systematically control changes to the system configuration during the system's life cycle. **{see Section 130 of the Certification Standards (Appendix G)}**	Documents should include policies and procedures that support the configuration management plan, including maintaining current configuration identification information; authorizing, testing, approving, and tracking all configuration changes; routinely auditing and verifying the configuration; updating software promptly to protect against known vulnerabilities; and approving emergency changes to the configuration.
4	Applicant has in place effective entity-wide policies and procedures at the system and application levels for segregation of duties. **{see Section 140 of the Certification Standards (Appendix G)}**	Documents should include policies and procedures that prevent one individual from controlling all critical stages of a process, and instead split the responsibilities between two or more organizational groups so that the likelihood is diminished that errors and wrongful acts will go undetected.

5	Applicant has in place effective contingency plans to prevent interruptions from resulting in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. **{see Section 150 of the Certification Standards(Appendix G)}**	Documents should include policies and procedures for protecting information resources and minimizing the risk of unplanned interruptions, as well as a plan for recovering critical operations should interruptions occur. The contingency plan should address the entire range of potential disruptions of a certified service provider. The contingency plan should: 1. Assess the criticality and sensitivity of computerized operations and identify supporting resources; 2. Take steps to prevent and minimize potential damage and interruption; 3. Be up to date and provide for alternate data processing, storage, and telecommunications facilities; and 4. Be tested periodically, the test results analyzed, and the contingency plan adjusted accordingly.
6	Applicant has a policy utilizing industry-standard availability/fault tolerance benchmarks. **{see Section 160 of the Certification Standards (Appendix G)}**	Plan to describe the redundancy, fail over capability, and availability of the system.
F	**Application Controls** **(Attach documentation to the application for all items requested in Section F)**	
1	Applicant has application level general controls ("application security") in place at the application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning. **{see Section 210 of the Certification Standards (Appendix G)}**	Documents should include evidence that the following exists: application security management plan, risk assessments; remediation of security weaknesses; external third party provider activities are secure, documented, and monitored; application users are appropriately identified and authenticated; public access is controlled; an access audit and monitoring program is in place; 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; changes to application functionality in production are authorized; unauthorized changes are detected and reported promptly; authorizations for changes are documented and maintained; changes are controlled as programs progress through testing to final approval; access to program libraries is restricted; access and changes to programs and data are monitored; there is segregation of duties between the security administration function of the application and the user functions; effective monitoring controls are in place to mitigate segregation of duty risks; application contingency planning includes a Business Impact Analysis (BIA) or equivalent; an application Contingency Plan exists and is periodically tested.

2	Applicant has in place a store-and-forward capability as backup to real-time mode.	Documents should include evidence that interactive systems between the Contractor and its sellers have been 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.
3	Applicant has business process (BP) controls in place that demonstrate the completeness, accuracy, validity and confidentiality of transactions and data during application processing. **{see Section 220 of the Certification Standards (Appendix G)}**	Documents should include policies and procedures related to transaction data input, transaction data processing, transaction data output, and master data setup and maintenance.
4	Applicant has in place the required predefined XML schemas, against which the transactions are validated, as well as appropriate restrictions on overriding and bypassing data validation and editing.	Documents should include policies and procedures demonstrating that the proper edits are in place, as well as restrictions on overrides to the system.
5	Applicant has appropriate interface controls are in place. **{see Section 230 of the Certification Standards (Appendix G)}**	Documents should include policies and procedures evidencing the implementation of effective interface strategy and design and interface processing procedures. Errors during interface processing are identified, investigated, corrected and resubmitted for processing. Rejected interface data is isolated, analyzed and corrected in a timely manner.
6	Applicant has in place sufficient data management system controls over the entry, storage, retrieval and processing of information, including detailed, sensitive information such as financial transactions, customer names, and social security numbers. **{see Section 240 of the Certification Standards (Appendix G)}**	Documents should include policies and procedures evidencing that the appropriate detective controls are in place, along with control capabilities over applications and/or functions not integrated into the applications.
7	Applicant has procedures and mechanisms to properly apply rounding rules **{see Section 324 of the Streamlined Agreement (Appendix G)}**	Copy of user/program specs and complete testing of the system.
8	Applicant maintains control mechanisms to provide assurance that the entry of erroneous data is captured, reported, investigated, and corrected **{see Section 220 (A) of the Certification Standards (Appendix G)}**	Copy of user/program specs and complete testing of the system. Also copies of error reports, files and logs. Policy as to how errors will be resolved.
G	**System Modification Accuracy** **(Attach documentation to the application for all items requested in Section G)**	
1	Applicant has procedures in place to provide assurance that only authorized and tested software modifications are made to the application system **{see Section 310 of the Certification Standards (Appendix G)}**	Copy of change control policies must include identification of individual access to files, and policy as to how programs are developed, changed, tested, and migrated into specific areas. Copies of approval forms, migration sheets, and test forms must be included.

2	Applicant has appropriate change control mechanisms to provide assurance that the appropriate level of software modification is matched to the data processed **{see Section 320 of the Certification Standards (Appendix G)}**	Copy of change control policies must include identification of individual access to files, and policy as to how programs are developed, changed, tested, and migrated into specific areas. Copies of approval forms, migration sheets, and test forms must be included.
H	**Sufficiency of Information** **(Attach documentation to the application for all items requested in Section H)**	
1	Applicant must demonstrate the system's ability to capture sufficient information to make an accurate tax determination **{see Section 400(A) of the Certification Standards (Appendix G)}**	This will be verified through the results from the system test process
2	Applicant has 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 and remitted **{see Section 400(A) of the Certification Standards (Appendix G)}**	Copy of procedures for connecting tax calculator with seller's system, including testing of seller transactions. For Applicants that rely upon their sellers to perform the mapping, review procedures provided to sellers on how to map taxable and exempt products and services.
3	Applicant's system has the ability to obtain, accumulate and report information on exempt sales **{see Section 400(B) of the Certification Standards (Appendix G)}**	Analyze test decks results for exempt sales. Provide a separate representation indicating an understanding of the Appendix F audit file requirements, including the detailed information it must contain.
4	Applicant implemented the proper use of state-provided sourcing information and compliance with state laws pertaining to taxability of tangible personal property and services **{see Section 400(C) of Certification Standards (Appendix G)}**	This will be verified through the results from the system test process
5	With the use of an audit trail, applicant has a method to track all changes to the system including sourcing, taxability and mapping of products in order to record all authorized and unauthorized changes, dates of changes, and changes to hardware, software, and software upgrades **{see Section 400 of the Certification Standards (Appendix G)}**	Policy on how changes are tracked
I	**Data Security** **(Attach documentation to the application for all items requested in Section I)**	
1	Mechanisms and procedures are in place to provide assurance that data exchanged between all parties is secure, non-repudiated, and unaltered **{see Section 500 of the Certification Standards (Appendix G)}**	Copy of policy describing type of security software, update sequence, and log of updates

2	For operational (transaction-related) data exchanged between a CSP and the Governing Board and the Member States, the appropriate standards are followed by applicant as set forth in the SST Certification and Auditing Standards documents **{see Section 500 of the Certification Standards (Appendix G)}**	Copy of policy describing type of security software, update sequence, and log of updates
3	For operational (transaction-related) data exchanged between a CSP and participating sellers, the appropriate standards are followed as set forth in the SST Certification and Auditing Standards documents **{see Section 500 of the Certification Standards (Appendix G)}**	Copy of policy describing type of security software, update sequence, and log of updates
4	For operational (transaction-related) data exchanged between a CSP and participating sellers, the appropriate transmission storage and virus protection is employed **{see Sections 550 and 560 of the Certification Standards (Appendix G)}**	Copy of policy describing type of security software, update sequence, and log of updates. Diagram of configuration of system.
5	A cyber security policy is in place. {see Sections 570 of the Certification Standards (Appendix G)}	Copy of policy describing processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Should include actions to be taken in response to security incidents.
6	A telecommuting policy is in place. {see Sections 570 of the Certification Standards (AppendixG)}	Copy of telecommuting policy for employees and subcontractors. Should include written telecommuting agreement, telecommuting safety checklist, and approval of mobile technology.
J	**Privacy Standards and Data Protection** **(Attach documentation to the application for all items requested in Section J)**	
1	Mechanisms and procedures are in place to provide assurance that confidential taxpayer information is adequately protected, consumers' privacy is protected and confidential and proprietary information is prevented from being sold or re-used in any way **{see Section 610 of Certification Standards (Appendix G), Section 321 of the Streamlined Agreement}**	Copies of security and personnel policy/procedures that indicate how confidential taxpayer information is protected, consumers' privacy is protected and confidential and proprietary information is prevented from being sold or re-used in any way. Copies of confidentiality forms and exit forms/procedures for terminating personnel.
2	Mechanisms and procedures have been implemented to provide assurance that personally identifiable information is protected **{see Section 620 of the Certification Standards (Appendix G), Section 321 of the Streamlined Agreement}**	Copies of security policy/procedures that indicate how confidential taxpayer information is protected, consumers' privacy is protected, and confidential and proprietary information is prevented from being sold or re-used in any way.

A motion by Kentucky on behalf of the Certification Committee to amend Appendix C (Sections E.6, I.5 and I.6) to make it consistent with Appendix G

K	**Electronic Format Capability and Sampling Procedures** **(Attach documentation to the application for all items requested in Section K)**	
1	Procedures have been implemented to provide unrestricted access to people performing the certification including remote access testing **{see Sections 210 (B) and 300 of the Certification Standards (Appendix G)}**	
2	Procedures and mechanisms have been established to provide access (either onsite or remote) to any documentation, system, database or system component, needed for them to perform the certification, re-certification, and audit **{see Section 700 of the Certification Standards (Appendix G)}**	