Secure Telephone Identity Policy Administrator RFP Respondent Qualification

Table of Contents

DISCLAIMER AND NOTICE

This Request for Proposal (RFP), including the associated Respondent Qualification and Technical Requirements Document (TRD), is published by the STI Governance Authority (STI-GA) to gather information that it expects to be useful in the selection of an STI Policy Administrator (STI-PA). However, the STI-GA makes no commitment to consider or purchase any offering or proposal from any party submitted in response to this RFP, or to take any action, including awarding a contract. The STI-GA reserves the right, at its sole discretion, to amend, delay, or cancel this RFP at any time for any reason.

Respondent bids must address all requirements applicable to the STI-PA in ATIS-1000074, ATIS-1000080, and ATIS-1000084 (the "ATIS SHAKEN Specifications") even if not addressed in the RFP. The STI-GA makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the information contained in this RFP, the ATIS SHAKEN Specifications, responses to questions submitted pursuant to this RFP, or any public or other materials describing the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. Any use or reliance on such information is at Respondents' risk. exchange for consideration of a Respondent's submission of questions or a proposal in response to this RFP, Respondent agrees by such submission to all of the terms of this RFP, including the limitations of liability and indemnification obligations set forth in Section 1.4.

The Respondent will bear all costs of preparing and submitting its proposal, responding to or providing any other assistance to the STI-GA in connection with this RFP.

Nothing contained herein shall be construed to confer any license or right to any intellectual property to any Respondent, whether or not the use of any information herein necessarily utilizes such intellectual property. The Respondent agrees that all documents, materials, articles, and information it submits with a question or as part of, or in support of a bid is and shall be given entirely voluntarily, and shall become, upon submission, the physical and intellectual property of the STI-GA in right that the STI-GA shall be free to use, disclose, and exploit as it sees fit, entirely without obligation or remuneration to the Respondent, and will not be returned to the Respondent at the conclusion of the RFP process.

1 General Project Information

1.1 Introduction

The FCC North American Numbering Council (NANC) Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR,[1] completed by the NANC Call Authentication Trust Anchor Working Group, recommended establishing an industry-led governance authority with broad representation from key industry associations and stakeholders. The identified stakeholders agreed to establish the Secure Telephone Identity Governance Authority (STI-GA) under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS). The NANC report also recommended that the Secure Telephone Identity Policy Administrator (STI-PA) should be selected through a Request for Proposal (RFP) process overseen by the STI-GA Board of Directors, the policy and decision-making body of the STI-GA.

The primary function of the STI-GA is to define, and modify as necessary, the rules governing the Secure Handling of Asserted information using toKENs (SHAKEN) framework. The STI-PA plays a key role in this framework, applying and enforcing the rules as defined by the STI-GA. In particular, the STI-PA verifies that a Service Provider (SP) meets the defined criteria for participation in the SHAKEN framework before issuing "Service Provider Code tokens" to the approved SP. The STI-PA must also renew the Service Provider Code token as required, after verifying that the SP continues to meet the criteria to participate in the SHAKEN framework. The Service Provider Code token is used for authentication when the SP obtains Secure Telephone Identity (STI) certificates from an approved Secure Telephone Identity Certification Authority (STI-CA). The STI-PA is also responsible for approving STI-CAs and verifying that the STI-CA meets all requirements of its Certification Practice Statement to assess compliance with Certificate Policy. Finally, the STI-PA must securely maintain a "trusted STI-CA" list and, when necessary, an SP certificate revocation list, and distribute this to all SPs participating in the SHAKEN ecosystem.

1.2 Purpose

This RFP is being issued by the STI-GA to identify a Respondent and/or any Sub-Contractor(s) (Respondent) that can design, develop, build, deliver, and operate the STI-PA function as defined in the ATIS SHAKEN Specifications ATIS-1000074, ATIS-1000080, and ATIS-1000084 (the "ATIS SHAKEN Specifications").

The chosen Respondent will be expected to deliver a secure, innovative, and efficient solution to securely manage the distribution of STI certificates to support the SHAKEN framework. The STI-PA function is envisioned to use existing, known, and proven technologies. However, no matter what solution the chosen Respondent provides, it must address all requirements.

The STI-GA will evaluate all proposals in order to select the Respondent and approach that best meets the requirements. However, the STI-GA makes no commitment to purchase any offering from a Respondent with respect to this RFP, or to take any action, including awarding a contract. The STI-GA assumes no contractual obligation, or specific contractual content by issuing this RFP, and reserves the right, at its sole discretion, to amend, delay or cancel this RFP at any time.

[1] The CATA WG's Final Report is available at: http://www.nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf

1.3 Respondent Qualification Response Instructions

This document is the second of three components in this RFP. Respondents should begin with the RFP component before completing this component.

The RFP process is comprised of three parts, which should be completed in this order and submitted together:

1. Secure Telephone Identity Policy Administrator Request for Proposal (RFP)
2. Secure Telephone Identity Policy Administrator RFP Respondent Qualification (Respondent Qualification)
3. Secure Telephone Identity Policy Administrator Technical Requirements Document (TRD)

Though the term RFP sometimes is used to refer solely to the first component, the term "RFP" encompasses all three components. The Respondent Qualification (this document) describes the criteria that must be satisfied by each prospective Respondent. This includes the Respondent's proposal, information about the Respondent's organizational structure, past performance, financial responsibility and stability, and acceptance of key business terms. The TRD describes the technical requirements for a proposal and the STI-PA's required obligations. Although great care has been taken to ensure the accuracy of the TRD and other reference documents, it is the Respondent's responsibility to ensure that any response to a specific technical requirement contained herein is based on the latest ATIS SHAKEN Specifications and other ATIS technical documents (available at http://www.atis.org/sti-ga/resources/) as well as other reference documents as currently published and made available to the industry.

Each Respondent is provided an opportunity to demonstrate how its proposal satisfies the RFP's requirements. Each Respondent is instructed to answer all questions in as concise and complete a manner as possible, and in many instances, the Respondent is provided with an opportunity to elaborate on its answers.

The STI-GA Board has authorized one of its Task Forces, the RFP Task Force (hereafter referred to as the RFP TF), to manage the STI-PA RFP process, including the solicitation and evaluation of responses. The selection process is expected to conclude in or about May 2019.

Please note:

1. Respondents must notify the STI-GA of their interest in bidding by e-mailing sti-ga@atis.org. Interested parties will be provided with credentials and instructions for bidding. E-mail, facsimile, or hard-copy responses will not be considered.

2. All questions must be emailed to sti-ga@atis.org and must be received no later than December 10, 2018. The STI-GA will endeavor to respond to all questions promptly and shall make answers available to all parties.

3. Respondents must satisfy the Respondent Qualification criteria and TRD criteria.

4. All responses and submissions must be complete, truthful, and accurate. Material misrepresentations or omissions may result in disqualification or reductions in scoring.

5. All responses must be received on or before the RFP response cut-off date as described in Section 1.5.

6. Nothing contained herein shall be construed to confer any license or right to any intellectual property to any Respondent, whether or not the use of any information herein necessarily utilizes such intellectual property.

7. When a Respondent prepares its quote and submits responses, the Respondent must review all specifications and drawings associated with a particular item, as the Respondent is responsible for quoting all material, performance, quality, and technical requirements for each individual item.

1.4 Terms Applicable to RFP Submissions

Respondents agree that all responses and information provided in connection with a response is given entirely voluntarily, and shall become, upon submission, the physical and intellectual property of the STI-GA in that the STI-GA shall be free to use, disclose, and exploit as it sees fit, entirely without obligation or remuneration to Respondent, and will not be returned to the Respondent at the conclusion of the RFP process. The STI-GA Board expressly reserves the right to reject any and all responses to this RFP. The STI-GA Board may engage independent consultants to assist in the evaluation of responses and to make recommendations to the STI-GA Board. The STI-GA Board reserves the right to request additional information or clarification from Respondents.

Responses must be submitted in accordance with the instructions in Section 1.3. Any response submitted after the RFP Cut-off Date as described in Section 1.5 of this RFP may not be considered. A Respondent is solely responsible for ensuring that its response is submitted and received by the STI-GA Board in accordance with the instructions.

The STI-GA makes no representation or warranty, express or implied, with respect to the completeness, accuracy or utility of the information contained in this RFP, the ATIS SHAKEN Specifications, responses to questions submitted pursuant to this RFP, or any public or other materials describing the SHAKEN framework. Any use or reliance on such information is at the Respondent's risk. In exchange for consideration of a Respondent's submission of questions or a proposal in response to this RFP, Respondent agrees by such submission to all of the terms of this RFP, including that the STI-GA Board (and Board Committees and Task Forces), ATIS and their employees, officers, agents, contractors, consultants, members, and counsel of each (each, an "Covered Party") shall not be liable to any entity for any damage, injury, or claim of lost opportunity incurred by any person arising out of the completeness, accuracy or utility of any information contained in this RFP or other information or any decision by the STI-GA to award or not to award a contract for the STI-PA role to any entity, and to indemnify and hold harmless each Covered Party from and against any and all liabilities, demands, damages, expenses and losses arising from such submission. These indemnification obligations and limitations of liability shall survive termination of the RFP and any contract executed in connection with the RFP. The Respondent shall be solely responsible for any claims, costs (including legal fees) or damages it incurs in connection with all submissions and responses.

In the event that the STI-GA engages a Respondent in discussions of its proposal that may lead to an agreement to serve as STI-PA, the Respondent may be required to agree to the terms of a confidentiality agreement to protect confidential information prior to the execution of the agreement to be executed between the STI-PA and STI-GA that will include confidentiality terms.

1.5 RFP Process Timeline

Below is the proposed time line for the Respondent selection pursuant to the RFP. The STI-GA reserves the right to modify or adjust the following dates or to otherwise change or amend this timeline:

- November 15, 2018: RFP issued and posted on STI-GA website.
- November 15, 2018: Press release published by ATIS on behalf of STI-GA.
- December 10, 2018: Last date to submit questions to STI-GA.
- February 4, 2019: RFP response cut-off date (deadline for bidders to submit proposals).
- May 2019: Selection of STI-PA by STI-GA.

Question 1

Respondent agrees that the submission of responses to this Respondent Qualification constitutes acceptance of all referenced and required terms and conditions set forth in this Respondent Qualification.

- Agree
- Disagree

2 General Respondent Company Information

Question 2

Please provide detailed information about the types of businesses or different lines of business in which the Respondent is engaged, including the percentages and revenues from each such type or lines of business. This information may also be attached.

- Attach file if necessary

Question 3

Please provide the following information about Respondent:

Company Name*	
Company Address 1*	
Company Address 2	
City, State and Zip Code*	
Primary Contact Name*	
Primary Contact Phone*	
Primary Contact Email*	
Secondary Contact Name	
Secondary Contact Phone	
Secondary Contact Email	

*Required

Question 4

Is the above address also the accounts receivable address for the Respondent? If not, please provide the accounts receivable address.

Question 5

Please provide details of the ownership and organizational structure, including affiliates and subsidiaries, of the Respondent, including a listing of all officers and members of the Board of Directors.

Question 6

How many years has the Respondent been in business? Has the Respondent ever done business under a different name(s), including mergers and acquisitions? If so, please provide the name(s).

Question 7

Is the Respondent publicly traded or privately held?

- Public company
- Private company

Question 8

If the Respondent is publicly traded, please provide the stock symbol and the exchange where the Respondent's stock is traded.

Question 9

What is the total number of employees of the Respondent?

3 Respondent Qualification Criteria

In order to be considered for the RFP, provide detailed responses to all the questions listed in this Section 3, *Respondent Qualification Criteria***.**

3.1 Financial Responsibility and Stability

In order to be recommended for selection under the RFP selection process as the STI-PA, a Respondent must possess sufficient financial responsibility and stability commensurate with the scope and duration of the services to be delivered pursuant to any agreement to be executed between the STI-PA and STI-GA. Please provide a concise description of the financial condition of the Respondent, if any, that the Respondent will engage or include in providing the services required by the RFP.

In addition to answering all questions in the Respondent Qualification, please attach:

- The most recent audited financial statements and annual report for the previous three (3) years of the Respondent and all such Sub-Contractor(s), if any.

- Responses must include all characteristics of the Respondent's (and all such Sub-Contractor(s)', if any) financial strength and wherewithal to demonstrate support that they can perform under a multi-year business contract of the magnitude and duration potentially to be awarded under the RFP.

Question 10

Please attach the financial information requested above.

- Attach file

3.2 Experience

In order to be recommended for selection under the RFP selection process as the STI-PA, a Respondent must possess sufficient experience, technical and operational capabilities to deliver the services required by the RFP in a timely, cost-effective, and technically and operationally proficient manner.

Provide a description of:

- Any relevant experience demonstrating a fundamental understanding of key management services that is performed in the U.S., or in other countries, that may be similar to the way the STI-PA is to be implemented within the U.S.

- Products and services offered, customers served, and successful performance of the functional/technical skills required on STI-PA activities performed for other customers (including contract duration, scope and order of magnitude of contract values).

- Any additional infrastructure that may be utilized to deliver STI-PA services.

These responses must include a concise description of the principal business of the Respondent, if any, including such items as company background, characteristics of business strength, and any

accomplishments and capabilities that demonstrate a strong foundation for managing and operating the STI-PA.

Question 11 Please attach a file providing a description of the information requested above.

- Attach file

Question 12

Identify and describe all threatened, pending, or concluded lawsuits or proceedings of any kind, (including but not limited to proceedings involving a governmental authority, whether federal, state, local, or foreign), during the immediately preceding five years asserting or involving terminations, breach or non-performance or deficient performance by the Respondent or its affiliates or any party that the Respondent has or would engage, under contracts, agreements or other arrangements.

- Attach file

Question 13

Provide three current client references that Respondent has been doing business with, for three years or longer. Include the client's/customer's official or registered name, nature of relationship, contact title, phone number, and email address. This information should be attached.

- Attach file

3.3 Acceptance of Key Business Terms and Conditions

Each Respondent submitting responses to the RFP must submit responses to this Respondent Qualification to identify which of the following key business terms and conditions that such Respondent, would agree to or not agree to if selected for recommendation as STI-PA to the STI-GA, by answering "Agree" or "Disagree" to each business term and condition. These terms and conditions are expected to be included in any agreement to be executed between the STI-PA and STI-GA. However, the following is not a comprehensive list of all contractual terms and conditions that may be included in any final and definitive agreements. The STI-GA Board reserves the right to change or add to the terms set forth herein prior to execution of any agreement to be executed between the STI-PA and STI-GA.

Question 14

The STI-PA shall provide the STI-GA Board all services and specified Service Level Requirements, and any agreement to be executed between the STI-PA and STI-GA, shall specify remedies and recourse for any failure by the STI-PA to provide the STI-GA Board the services at or above the Service Level Requirements. These remedies and this recourse may include monetary Performance Credits, price reductions, and, in certain specified circumstances, termination.

- Agree
- Disagree

Question 15

The STI-PA shall monitor its compliance with all Service Level Requirements specified in any agreement to be executed between the STI-PA and STI-GA and the Methods and Procedures (M&Ps) documents and certain other specified requirements and functionalities set forth in any agreement to be executed between the STI-PA and STI-GA and issue reports on such compliance at specified periodic intervals.

Additionally, by submitting a response to the RFP, the Respondent understands and agrees that any changes to the specifications subsequent to the issuance of the RFP and prior to the turn- up of the system described in the RFP, MUST be incorporated into the proposed system platform and ready for implementation at turn-up as part of the services to be offered under any agreement to be executed between the STI-PA and STI-GA .

- Agree
- Disagree

Question 16

The STI-GA Board shall have the right to terminate any agreement to be executed between the STI-PA and STI-GA entered into through this RFP with the STI-PA for reasons of default as defined in any agreement after a specified cure period has passed. These reasons include, but are not limited to, an adverse change in the financial stability of the STI-PA, including receivership, bankruptcy or assignment for the benefit of creditors, or for any reason or under circumstance required by or related to a change in the law or regulations requiring such termination. Upon such termination, unless transition services are provided as required below, users shall be responsible for paying the STI-PA only for services performed prior to such termination. The STI-GA Board shall have absolutely no liability for any payments to the STI-PA.

- Agree
- Disagree

Question 17

Upon termination for any reason or non-renewal at the conclusion of the term of any agreement to be executed between the STI-PA and STI-GA, the STI-PA shall agree to cooperate with the STI-GA Board, if requested, to effect the orderly transition of services to a successor STI-PA by providing specified transition services for a specified period at reasonable rates consistent with the charges in effect prior to termination or non-renewal.

- Agree
- Disagree

Question 18

The STI-GA Board shall be granted appropriate license rights in and to any technology or other intellectual property that is developed for and at the request of STI-GA Board for the STI-PA function and for the purposes of providing the services. The Respondent shall agree to appropriate limitations on

their use of any such technology or other intellectual property for purposes other than the express provision of the services.

- Agree
- Disagree

Question 19

In the event of termination or non-renewal of any agreement to be executed between the STI-PA and STI-GA, the Respondent shall for a specified time deposit all technology and other intellectual property (including Source Code and Object Code) and related documentation under its control, that is necessary to the operation of the STI-PA functions and the provision of these services, including all billing and collections functions, with a mutually agreeable escrow agent for release to and the use by the STI-GA Board (or its agents or contractors) as a nontransferable licensee, or to allow a successor STI-PA as a nontransferable licensee, the ability to operate the STI-PA and to provide services.

- Agree
- Disagree

Question 20

The STI-PA shall, at its own cost and expense, obtain and maintain all licenses, authorization, permits and permissions required by applicable legislative enactment and regulatory authorizations necessary to operate and maintain the STI-PA functions and to offer the services, to pay all taxes incident thereto (including but not limited to, all applicable sales and use taxes and levies) and to comply with all applicable federal, state, county and local laws, ordinances, regulations and codes in the performance of the obligations under any agreement to be executed between the STI-PA and STI-GA, including but not limited to the compliance with all laws, regulations, rulings, and ordinances with respect to immigration and export controls. The STI-PA shall maintain and implement an export compliance program and other compliance programs as needed to assure compliance with applicable laws.

- Agree
- Disagree

Question 21

The Respondent chose as the STI-PA shall be required during the term of any agreement to be executed between the STI-PA and STI-GA to provide any enhancements, additions and changes to the system and to the services pursuant to specific Statements of Work or other means in accordance with a procedure and process set forth in any agreement to be executed between the STI-PA and STI-GA .

- Agree
- Disagree

Question 22

The Respondent chosen as the STI-PA shall be responsible for providing disaster recovery and backup plans with respect to the data centers sufficient to ensure that all data is recoverable at all times. In the event of a disaster, the Respondent chosen as the STI-PA shall not increase its charges under any

agreement or charge usage fees or other charges in addition to the fees otherwise payable under any potential agreement to be executed between the STI-PA and STI-GA. Such disaster recovery and backup process shall be subject to audit and periodic testing.

- Agree
- Disagree

Question 23

Data centers, servers and user data must be maintained and stored in the U.S. No data relating to any such service will be stored, at, in, or through a site located outside of the U.S.

The Respondent must agree and commit that it will not store, maintain, or warehouse, user data in a physical or electronic form, on servers or otherwise, at any location that is not within the U.S.

- Agree
- Disagree

Question 24

The Respondent must agree and acknowledge that the STI-GA Board is not granting any exclusive right to provide services.

- Agree
- Disagree

Question 25

The Respondent must agree that user data shall be maintained as confidential information and may not be used or commercially exploited in any manner other than for the performance of the STI-PA's obligations under any agreement to be executed between the STI-PA and STI-GA, subject to certain regulatory or legal requirements or, in certain cases, upon the consent of the STI-GA Board.

- Agree
- Disagree

Question 26

The STI-PA will be expected to agree to indemnify and hold harmless the STI-GA Board and ATIS and their members, parents, subsidiaries, other affiliates, direct and indirect customers, and the officers, directors, employees, successors, agents, consultants, representatives, attorneys and counsel, successors and assigns of any and all of them (collectively, the "Indemnified Parties"), from and against any and all claims, losses, damages, expenses, liabilities, suits, demands, causes of action, including costs and reasonable attorney's fees, or liens, including without limitation, those based on contract or tort, that arise out of or result from any or all of the following:

i. Injury or death to persons, or loss or damage to any and all property, including theft, in any way arising directly or indirectly out of, or occasioned by, caused or alleged to have been caused by, or on account of, the performance as the STI-PA, or its sub-contractor(s), if any, or its agents, or

any director, officer, employee, agent or representative under the RFP, or the agreement to be executed between the STI-PA and STI-GA;

ii. Assertions under Workers Compensation or similar acts made by persons furnished by or employed by the STI-PA or sub-contractor(s), if any, or by reason of any injuries to such persons; and

iii. Any failure on the part of the STI-PA, or sub-contractor(s), if any, to satisfy all claims for labor, equipment, materials and other obligations relating to the performance under the agreement to be executed between the STI-PA and STI-GA.

The Respondent chosen as the STI-PA must agree to defend or settle, at its own expense, any action or suit asserted against the Indemnified Parties, including all proceedings involving income, sales, use, or other taxes, and shall reimburse the Indemnified Parties for reasonable attorneys' fees, interest, costs of suit and all other expenses incurred by the Indemnified Parties in connection therewith.

- Agree
- Disagree

Question 27

The Respondent chosen as the STI-PA on behalf of itself and all sub-contractor(s), if any, will defend or settle, at its own expense, any and all claims and suits against any of the Indemnified Parties alleging that any products or services furnished pursuant to any agreement to be executed between the STI-PA and STI-GA, including any portion of the services, infringe or constitute a misappropriation of any patent, trade secret, copyright, or proprietary interest. The Respondent will also pay all damages and costs that by final judgment or settlement may be assessed against or chargeable to any of the Indemnified Parties due to such infringement or misappropriation.

If a Respondent's products or services, including any portion of the services, become, or in the STI-GA Board's opinion are likely to become, the subject of a claim of infringement, the Respondent will, at its option: (1) procure for the STI-GA Board the right to continue using the applicable product or service or (2) replace or modify the product or service to provide the STI-GA Board with a non-infringing product or service that is functionally equivalent in all material respects.

- Agree
- Disagree

Question 28

During the term of any agreement to be executed between the STI-PA and STI-GA, the Respondent chosen as the STI-PA shall obtain and maintain, with financially reputable insurers (i.e., carriers with an A.M. Best rating of A- :VIII, or better) that are licensed to do business in all jurisdictions where any work is performed or the services are provided and which are reasonably acceptable to STI-GA Board, not less than the following levels of insurance coverage for each Region for which an RFP Contract is awarded:

i. Worker's Compensation insurance coverage as provided for under any worker's compensation or similar law in any jurisdiction where any work is performed, of not less than the minimum required coverage amount required under the law of any jurisdiction where work is performed, and Employer's Liability insurance coverage of at least $500,000 per each occurrence and in the aggregate.

ii. Commercial general liability insurance coverage, including coverage for contractual liability and products/completed operations liability, with a limit of not less than $1,000,000 combined single limit per occurrence for bodily injury, property damage and personal injury liability (with contractual exclusion deleted) and in the amount of at least $2,000,000 in the general aggregate, naming STI-GA Board, its members, their directors, officers, employees, agents and/or representatives as additional insured.

iii. Business auto liability insurance coverage covering the ownership, maintenance or use of any owned, non-owned or hired automobiles with a limit of not less than $1,000,000 combined single limit per accident for bodily injury and property damage liability, naming STI-GA Board, its members, their directors, officers, employees, agents and/or representatives as additional insured.

iv. Umbrella/excess liability insurance coverage with limits of not less than $15,000,000 combined single limit in excess of the above-referenced employer's liability insurance coverage, commercial general liability insurance coverage and business auto liability insurance coverage naming STI-GA Board, its members, their directors, officers, employees, agents and/or representatives as additional insured.

v. "All Risk" Property insurance coverage covering not less than the full replacement cost of all data centers and personal property at risk, including business interruption or continuation insurance coverage sufficient to allow a Respondent to continue to satisfy its obligations as an STI-PA under the agreement to be executed between the STI-PA and STI-GA during the period of any covered loss.

vi. Errors and omissions liability insurance coverage in the amount of at least $20,000,000 per claim with an annual aggregate of at least $20,000,000 inclusive of legal defense costs.

Neither the Respondent chosen as the STI-PA nor its insurer(s) shall have a right of subrogation against the STI-GA Board based on any loss or liability insured against under the foregoing insurance. Policies for the above-referenced insurance must be endorsed to name the STI-GA Board as an additional insured and state: "STI-GA Board is to be notified in writing at least thirty (30) days prior to cancellation of or any material change in the coverage limits." Also, the Respondent chosen as the STI-PA must furnish certificates evidencing the foregoing insurance coverage within thirty (30) days following execution of any agreement to be executed between the STI-PA and STI-GA and prior to the commencement of any work and prior to the renewal thereof, in form and content to STI-GA Board, evidencing that the above insurance is in force and contains a provision that it will not be canceled or materially altered without

first giving STI-GA Board thirty (30) days prior written notice and that all coverage is primary to any insurance carried by STI-GA Board or its embers.

Nothing contained in this section shall limit the Respondent chosen as the STI-PA's liability to STI-GA Board to the limits of insurance coverage certified or actually carried.

- Agree
- Disagree

Question 29

A Respondent shall submit a list of all Sub-Contractor(s), if any are to be engaged by the Respondent to STI-GA Board with its Proposal. Any subsequent change in the use of any Sub- Contractor(s) shall require the review and approval of STI-GA Board.

- Agree
- Disagree

- Attach file if necessary

Question 30

The Respondent chosen as the STI-PA shall not have the right to assign any obligations, rights, duties or responsibilities under any agreement to be executed between the STI-PA and STI-GA, without the prior written approval of the STI-GA Board. The STI-PA shall not have the right to assign or to pledge any monies due or accounts received under any Statement of Work (SoW) or any agreement to be executed between the STI-PA and STI-GA without the prior written approval of the STI-GA Board.

- Agree
- Disagree

Question 31

In the event that the deployment of the Policy Administration function or any aspect of the service does not pass a mutually agreed upon Acceptance Plan set forth in any agreement to be executed between the STI-PA and STI-GA, designed to determine the STI-PA's compliance with the functional and technical requirements of the ATIS SHAKEN Specifications and any potential agreement, the STI-GA Board shall have the option to terminate any agreement without any penalties whatsoever to it or its members, and their parents, subsidiaries, other affiliates, their direct and indirect customers and any users, and the officers, directors, employees, successors, agents, consultants, representatives, attorneys and counsel, successors and assigns of any and all of them and the STI-PA shall be liable for liquidated damages in the amount to be specified in which the agreement to be executed between the STI-PA and STI-GA is terminated.

- Agree
- Disagree

Question 32

The STI-PA, on behalf of itself and any sub-contractors must agree to the following limitations on liability under any agreement to be executed between the STI-PA and STI-GA:

Neither party shall be liable to the other for any indirect, punitive, special, or consequential damages arising out of or in connection with any agreement to be executed between the PA and STI-GA, the user agreements or any SoW or the performance or non-performance of obligations undertaken. Each party waives any claim to such damages against the other.

The limitations or exculpations of liability set forth in the first sentence will not be applicable to:

i. Indemnification claims.
ii. Liability resulting from the gross negligence or willful misconduct of a party.
iii. Any breach of a party's confidentiality obligations

- Agree
- Disagree

4 Overview of Respondent Proposal

In addition to all other requirements, the Respondent shall propose the following plans:

- A business plan ("Respondent Business Plan")
- An implementation plan ("Respondent Implementation Plan")
- An operational plan ("Respondent Operational Plan")
- A detailed security plan ("Respondent Security Operational Plan")
- A statement of work ("Respondent SoW")
- Proposed Service Level Requirements ("Respondent SLR")
- A proposed statement of limitations, including liability ("Respondent Limitation of Liability")
- A statement disclosing any potential conflicts of interest ("Conflict of Interest Statement")

4.1 Respondent Business Plan

The Respondent Business Plan must clearly show how the Respondent intends to build a sustainable business around the STI-PA operation and corresponding business model. Among other important business drivers, the plan should include all revenue and cost assumptions (including all start-up and initial costs, expenses, and fees) and a pricing model through 2024 (five (5) years, starting 2019).

Question 33

Please attach a Business Plan.

- Attach file

4.2 Respondent Implementation Plan

The Respondent Implementation Plan should describe the Respondent approach to design, develop, implement, and test the proposed implementation plan.

Question 34

Please attach an Implementation Plan:

- Attach file

4.3 Respondent Operational Plan

The Respondent Operational Plan should address the requirements listed in this section.

The Respondent must be a legal entity formed and based in the United States authorized to do business in all 50 States. At no time shall the Respondent maintain, use, transmit, or cause to be transmitted confidential information outside the United States and its territories.

The platforms deployed to support the operation of the STI-PA, and any backup data associated with these platforms, must be located in the U.S. The platforms and APIs deployed to support the operation of the STI-PA must only be accessed from within the U.S. by authorized STI-PA employees, SPs, and STI-CAs unless explicitly authorized by the STI-GA. All functionality related to these platforms, whether contemplated by this RFP, or as set forth in the future, must be limited to within the US unless explicitly authorized by the STI-GA.

The STI-GA is not liable for any work performed by the Respondent or Respondent´s subcontractor(s) related to this RFP.

4.3.1 Operations and Administration

The Respondent is responsible for the operations and administration of all required functions to support the role of the STI-PA. The response should at a minimum address:

- Roles and responsibilities.
- Budgeting and financial management.
- Organization, staffing, and training.
- Facilities, utilities and technology.
- Performance improvement and tracking.
- Privacy and security.
- A date by which the Respondent can commit to be able to make all STI-PA functions and services available.

4.3.2 Maintenance

The Respondent is responsible for the maintenance of all required equipment, software, and facilities necessary to execute the role of the STI-PA. This includes all licenses, and all technology and tools needed to successfully execute the intended business functions and comply with all Requirements. The Respondent is responsible for all costs, expenses, and fees related to the upkeep, maintenance, and upgrades of any equipment, software, and facilities required by the platforms deployed to support the operation of the STI-PA:

- Condition-based maintenance
- Corrective maintenance
- Planned maintenance
- Predictive maintenance
- Preventive maintenance

4.3.3 Availability, Reliability, and Resiliency Reporting

The Respondent is responsible for reliable operation of the STI-PA function. This includes ensuring the service is available, reliable, and resilient to deliver services in accordance with the planned uptime of the system. The Respondent should include in its response sufficient details in its SLR to evaluate this requirement. Section 6 of the RFP provides minimum requirements.

4.3.4 Reporting, Audit and Data Analytics

The STI-PA will be responsible for data management, as well as performing internal analysis and reporting as it relates to execution of the STI-PA role. The same analysis and reporting structure need to be sufficiently flexible enough to address new requirements in a cost effective and timely manner.

- Audit Provisions: The STI-PA will be subject to yearly procedural and financial audits to ensure proper implementation of any agreement to be executed between the STI-PA and STI-GA. The STI-PA is expected to engage an independent auditor to review the Respondent’s controls surrounding the STI-PA function and to submit the auditor’s opinion to the STI-GA.

4.3.5 Contingency Recovery Plans

Detailed contingency planning process for response to possible catastrophic events (e.g. acts of nature, act of men) or system failures are required and should be included in the RFP response.

Question 35

Please attach an Operational Plan as outlined in Section 4.3:

- Attach file

4.4 Respondent Security Operational Plan

The Respondent must submit a Respondent Security Operational Plan that clearly outlines how the Respondent will adhere to the required security practices related to the STI-PA's technical, operational, and administrative functions. This section sets forth elements of a Respondent Security Operational Plan.

While the Respondent's proposal should address the elements described in the sections on Data Protection and Cybersecurity below, these elements may be subject to change depending on the legal, regulatory, and business needs of the STI-GA. In the event that Respondent is selected, the Respondent will work with the STI-GA and its Technical Committee, as needed, to further develop, supplement, or modify the Respondent's Security Operational Plan to meet the required privacy and security practices.

The STI-GA is open to various storage methods for Service Provider Code tokens, CA Lists, and other stored information necessary to execute the role of the STI-PA, provided that all storage proposals are fully compliant with the Security Operational Plan.

4.4.1 Data Protection

In order to minimize the potential for unauthorized access, loss of data or other misuse of the STI-PA Information, the Respondent must plan and implement a comprehensive written privacy and cybersecurity program with controls and processes that protect the platforms deployed to support the operation of the STI-PA from threats, both internal and external. These privacy controls and processes should include, but are not limited to:

4.4.1.1 Data Management and Governance

Respondent defines, documents, communicates, and assigns accountability for its privacy policies and procedures. This includes:

- Designating a senior-level employee or employees to: (1) coordinate and be responsible for the Respondent Security Operational Plan; and (2) educate Respondent employees and agents about the importance of the appropriate protection and use of STI-PA, STI-CA, and SP information.

- Conducting periodic privacy risk assessments to identify reasonably foreseeable, material risks, both internal and external, that could result in the unauthorized collection, use, or disclosure of STI-PA, STI-CA, and SP Information, and the sufficiency of safeguards in place to control those risks.

- Designing and implementing internal controls and procedures to address identified security risks, and the regular testing or monitoring of the effectiveness of those controls and procedures.

- The periodic evaluation and adjustment of the Respondent Security Operational Plan in light of: (1) the results of the testing and monitoring of security controls; (2) evolving best practices; (3) any material changes to Respondent's operations or business arrangements; or (4) any other circumstances that Respondent knows, or has reason to know, may have a material impact on the effectiveness of the Respondent Security Operational Plan.

- Clear consequences for any personnel who violate policies and procedures related to STI-PA, STI-CA, or SP information.

4.4.1.2 Process for Collecting and Using Sensitive Data

Respondent has additional protective procedures when collecting and using sensitive categories of STI-PA, STI-CA and SP information, to the extent it collects or uses such information.

4.4.1.3 Internal Access Controls

Respondent implements procedures to manage access to STI-PA, STI-CA and SP information in a manner that is reasonably designed to limit access to authorized individuals, including: (1) role-based access permissions; (2) provisioning and de-provisioning procedures; (3) adopting classifications to segment data; (4) where possible, implementing the principle of least access; and (5) periodically auditing access permissions.

4.4.1.4 Third-Party Disclosures

Respondent implements appropriate measures and controls designed to restrict access to STI-PA, STI-CA, and SP information or other data held by the STI-PA from third-party disclosure, unless the extent of such access is explicitly authorized by STI-GA. In the event that the STI-GA approves the Respondent request to disclose STI-PA, STI-CA or SP information to a third party, the Respondent shall (1) evaluate the capacity of the third party to appropriately protect the security of the information, as applicable, and (2) contractually require the third party to implement and maintain appropriate security protections. After entering into the relationship, the Respondent periodically assesses the ability of the third party to appropriately protect the security of STI-PA, STI-CA, and SP information. With respect to third party disclosures involving governmental authorities or legal process, the Respondent adopts procedures to respond to criminal and civil legal process.

4.4.1.5 Personnel Management and Training

Respondent manages operational risk associated with personnel who have access to STI-PA, STI-CA, or SP information, including: (i) conducting appropriate background checks; (ii) factoring security into procedures for onboarding and off boarding personnel; and (iii) providing security training for personnel with access to STI-PA, STI-CA, or SP information that covers the security program, emphasizes the importance of compliance with security obligations, highlights relevant security risks, and provides guidance about how to mitigate security risks. Training must be provided to all employees who access any STI-PA, STI-CA, and SP information.

4.4.1.6 Incident Management and Response Plan

The Respondent provides personnel with clear responsibilities and guidance regarding the investigation, resolution, and documentation of reported and identified incidents and vulnerabilities impacting STI-PA,

STI-CA, and SP information, including data breaches and possible use of information in violation of security policies. The Respondent has a written incident response plan addressing unauthorized access to STI-PA, STI-CA, or SP information. STI-PA also has a process to notify STI-GA promptly regarding any non-compliance with the Respondent Security Operational Plan or applicable security legal requirements.

4.4.1.7 Data Retention

The Respondent has appropriate data retention policies to retain STI-PA, STI-CA, and SP information for business and legal purposes. The Respondent also has procedures to dispose of or de-identify information, taking into account litigation hold procedures and other exceptions.

4.4.1.8 Acceptable Use

The Respondent adopts appropriate restrictions on internal communications and the use of electronic resources (such as through a code of conduct or acceptable use policy) to protect STI-PA, STI-CA, and SP information.

4.4.1.9 Employee Monitoring and Bring-Your-Own-Device

The Respondent describes and complies with applicable legal restrictions on the monitoring of employee use of internal communications and electronic resources.

4.4.1.10 Plan Auditing

The Respondent has sufficient auditing mechanisms in place for STI-GA to review and assess the sufficiency of the Respondent Security Operational Plan.

4.4.1.11 Additional Privacy Plan Components

To the extent not already discussed above, the Respondent Security Operational Plan may incorporate additional measures.

4.4.2 Cybersecurity

A comprehensive data protection program is complemented by a comprehensive cybersecurity program that is reasonably designed to protect STI-PA, STI-CA, and SP information from unauthorized access, use, disclosure, and loss. The Respondent is expected to implement a cybersecurity risk management plan that is a flexible and dynamic enough to adapt to new threats, systems, users, and other alterations in the SHAKEN/STIR ecosystem throughout the data life cycle.

The foundation for the cybersecurity program should minimally include items as outlined below. The program should also incorporate, as a minimum, applicable standards from NIST, CSRIC, and ISO. In addition, communications involving STI-PA, STI-CA, and SP information shall be encrypted while in transit. All stored STI-PA, STI-CA, and r SP information shall also be encrypted while stored (“at rest”).

1. Identify/Discover
    a. Inventory all existing systems and applications on a periodic basis
    b. Classify the assets
    c. Identify owners
    d. Discover and routinely scan for existing vulnerabilities
2. Assess/Prioritize
    a. Conduct risk assessments

b. Establish security controls
c. Develop remediation plans
d. Prioritize activities and investments

3. Implement/Operate
   a. Administer additional controls
   b. Execute remediation plans
4. Monitor/Analyze
   a. Scan and patch vulnerabilities
   b. Ensure latest version software and firmware
   c. Monitor threat developments through information sharing activities/services
   d. Log events, including authentication events
   e. Manage and log privileged account usage and events
   f. Capture metrics
5. Test/Evaluate
   a. Audit on a routine basis
   b. Control and improve effectiveness of plans and procedures
   c. Conduct third-party audits and trusted penetration testing
   d. Establish contingency plans (Business Continuity Plan/Disaster Plan)
6. Improve/Evolve
   a. Reassess risks and vulnerabilities
   b. Re-evaluate policies, procedures and plans at least annually
7. Train/and raise Awareness
   a. Ensure periodic user training
   b. Conduct periodic incident response exercises and incorporate lessons learned

Question 36

Please attach a Security Operational Plan as outlined in Section 4.4.

- Attach file

4.5 Respondent SoW

The Respondent must submit a SoW that will clearly articulate the specific work items that the Respondent will perform in order to satisfy the requirements of the RFP.

Question 37

Please attach a SoW.

- Attach File

4.6 Respondent Service Level Requirements (SLR)

The Respondent must submit SLR(s) that will clearly articulate the service level categories and corresponding attributes for interactions between the STI-PA and the SPs and/or STI-CA.

Question 38

Please attach the SLR(s).

- Attach File

4.7 Respondent Statement of Liability

The Respondent must submit a statement that identifies any and all limitations on its own liability that it believes are necessary to be included in any agreement to be executed between the STI-PA and STI-GA, if awarded.

Question 39

Please attach the Statement of Liability.

- Attach File

4.8 Respondent Conflict of Interest Statement

The Respondent must submit a separate statement that clearly discloses any potential conflicts of interest that Respondent, or any subcontractor that Respondent engages in relation to the RFP, have in performing these services for the STI-GA.

Question 40

Please attach a Conflict of Interest Statement.

- Attach File

4.9 Business Continuity Plan Requirements

REQ 1: The STI-PA shall have a Business Continuity Plan that will be executed in case of severe service disruptions due to a catastrophic event (fire, act of nature, war, etc.), as more fully to be described in the agreement to be executed between the STI-PA and STI-GA. A service disruption could result from, but not limited to, a loss of key personnel, loss of facilities, and loss of critical IT functions.

REQ 2: The STI-PA shall, at its sole expense, shall conduct periodic unannounced Business Continuity Plan Exercises that are non-service impacting to assure that employees understand and follow the Business Continuity Plan and to assess the adequacy of the Business Continuity Plan.

REQ 3: The STI-PA shall, at its sole expense, prepare and deliver to the STI-GA Board a written report regarding the conduct and results of each Business Continuity Plan Exercise, including a specification of corrective actions and anticipated timelines for implementation, if any.

Question 41

Please attach a copy of an existing Business Continuity Plan in use by the Respondent.

- Attach File

Question 42

Does Respondent fully agree to conduct and implement a Business Continuity Plan, including Business Continuity Plan Exercises, as outlined above?

- Agree
- Disagree