Input to Draft FCC KYUP *FNPRM*

WT Docket No. 17-97, GC Docket No. 17-99

Thomas Goode, ATIS General Counsel
Brent Struthers, STI-GA Director
Glenn Clepper, STI-GA Board Chair
Gunnar Halley, STI-GA Board Vice-Chair
John Marinho, STI-GA Board Director
Michael Starkey, STI-GA Board Director
Courtney Tolerico, CTIA

May 13, 2026

Input to the Draft KYUP *FNPRM*

- The STI-GA and the IPNNI Task Force support the FCC's commitment to combating illegal robocalls and protecting American consumers from unlawful and fraudulent calling activity. STIR/SHAKEN remains a critical tool in this effort, and the STI-GA is dedicated to the continued integrity and effectiveness of the framework.
  - We welcome the opportunity to engage with the Commission and appreciate the ongoing dialogue.
  - In reviewing the draft *FNPRM*, the STI-GA has identified a number of factual inaccuracies and mischaracterizations that, if left uncorrected, could undermine the record and lead to misguided regulatory outcomes.
- The following fact-based comments are intended to correct the record; they reflect input from:
  - The Joint ATIS-SIP Forum Internet Protocol Network to Network Interconnection Task Force (IP-NNI Task Force), which develops and maintains the Signature-based Handling of Asserted Information using toKENs (SHAKEN) series of standards.
  - STI-GA Board, which establishes and governs the policies and the security around issuance and use of STI certificates by SHAKEN participants in the U.S. ATIS is submitting the input on behalf of the STI-GA Board.

STI-GA and IP-NNI Task Force Input

- **Issue**: The questions in Paragraph 64 about delegate certificates appear to be based on misunderstanding of the existing certification framework. STI-PA authorization of enterprises or end users is not required for those entities to obtain delegate certificates. Delegate certificates are not issued by the STI-CA. Delegate certificates establish a verified association between the end user customer and the telephone number that is being used by a service provider to originate the call when that service provider did not issue the telephone number.
- ***Proposed Edit to*** **Paragraph 64**:
  - "Should we further find that delegate certificates are a viable method for originating providers to establish a verified association between an end user customer, such as a non-voice service provider enterprise, and the number being used to initiate the call. ~~If so, does the Governance Authority need to modify its SPC token policy so that such end users can obtain SPC tokens and certificates? What are the risks and benefits of allowing non-provider entities to have a role in the STIR/SHAKEN ecosystem?~~"

STI-GA Input

- **Issue**: Paragraph 12 of the draft *FNPRM* erroneously implies that the STI-GA's role is broader than it is. The STI-GA's purview is limited to the STIR/SHAKEN call authentication ecosystem, not the entire voice ecosystem.
- **Proposed Edit to Paragraph 12**:
  - "Similarly, the STIR/SHAKEN Governance Authority was designed to maintain trust in the STIR/SHAKEN framework by setting policies and procedures that govern the assignment of digital certificates used by providers to authenticate calls within ~~which providers may be a part of~~ the voice ecosystem."

STI-GA Input (cont'd)

- **Issue**: Paragraph 46 asks about requiring the STI-GA to adjust its certificate issuance policy to establish a maximum expiration timeline for STI certificates. However, the STI-GA Certificate Policy, Section 6.3.2, already sets a maximum lifetime of 3 years for the STI certificate, and many STI-CAs set a shorter maximum lifetime. With regard to SPC tokens, in 2023, the STI-GA authorized a software change to the STI-PA systems that set the maximum lifetime for an SPC token at two weeks.
- **Revise the last sentence in Paragraph 46 to read as follows:**
  - "Should we also require the Governance Authority to adjust the certificate issuance policy, such as by changing the ~~establishing a~~ maximum expiration timeline for STI certificates?"

STI-GA Input (cont'd)

- **Issue:** Paragraph 47 seeks comment on the STI-GA conflicts of interest (COI) policy. The *FNPRM* mischaracterizes the STI-GA's COI policy as it relates to Certification Authorities. The current policy guards against conflicts due to "common ownership" rather than due to "close relationships" and warrants clarification, as it does not specify which "providers" are contemplated and may be read more broadly than intended. Certification Authorities enter into contracts and terms of use with service providers as part of the certificate issuance process, which inherently involves a close business relationship as a supplier to the Service Provider. Striking the language "or having a close relationship with providers," would narrow the provision to address potential conflicts of interest. As an alternative, the FCC could insert "common ownership" to avoid encompassing all legitimate close relationships with providers.
- **Proposed Edit to Paragraph 47**:
  - "Although the Governance Authority has established a policy concerning conflicts as to a Certification Authority also serving as the Policy Administrator, it has not Established a conflict-of-interest policy as to a Certification Authority also acting as a provider or having ~~a close relationship~~ common ownership with providers for which the Certification Authority issues certificates. We are concerned about such relationships because a Certification Authority may have incentive to issue certificates to providers to which they are related without following the certificate issuance policy. We seek comment on this assessment."

STI-GA Input (cont'd)

- **Issue:** Paragraph 48 of the draft incorrectly states that the STI-GA has only revoked SPC tokens for providers that have failed to pay required fees or failed to supply annual FCC Form 499 revenue data. As has been previously reported to the FCC staff, revocations have occurred for other reasons as well, including due to RMD removals and/or deletions, FCC final determinations, improper attestations and voluntary surrenders.
- **Delete the following from Paragraph 48:**
  - ~~"Despite well-known reports that providers are applying improper attestations to calls or otherwise failing to follow the STIR/SHAKEN standards, the Governance Authority has reported to Commission staff that it has only revoked SPC tokens for providers that have failed to pay required fees or failed to supply annual FCC Form 499 revenue data, which the Governance Authority uses to calculate fees.~~"

STI-GA Input (cont'd)

- **Issue:** Paragraph 49 references violations of the STI-GA's certificate issuance policy but fails to provide citations to the specific provisions that are believed to have been violated. As STI-CAs have no control or knowledge of how a service provider makes use of its certificate once assigned, there is no STI-GA policy that ties Certification Authorities to the manner in which service providers use their certificates.
- **Delete the Fifth Sentence in Paragraph 49:**
  - "Anecdotally, the Commission staff ~~has learned~~ is concerned that certain Certification Authorities issue a disproportionate number of certificates that are being used by voice service providers applying improper attestations to their calls. ~~We believe this is indicative of Certification Authorities not following the Governance Authority's certificate issuance policy.~~"

Questions?

Thomas Goode
ATIS General Counsel
tgoode@atis.org

John Marinho
STI-GA Board Director
JMarinho@ctia.org

Brent Struthers
STI-GA Director
bstruthers@atis.org

Michael Starkey
STI-GA Board Director
mstarkey@qsiconsulting.com

Glenn Clepper
STI-GA Board Chair
Glenn.Clepper@charter.com

Courtney Tolerico
CTIA
ctolerico@ctia.org

Gunnar Halley
STI-GA Board Vice-Chair
gunnarh@microsoft.com

ADVANCING INDUSTRY TRANSFORMATION

www.atis.org

Supplementary Information - Recommended Changes to Draft *FNPRM*

Proposed Edit to Paragraph 64

(footnotes omitted)

64. To resolve these practices, we propose two mechanisms that providers may use to establish a customer's association with a number. First, we propose to find that an originating provider may establish a verified association between its customer and the telephone number used when the originating provider is the TNSP (i.e., it assigned the telephone number to the customer either as an individual number or as part of a range of numbers).140 Second, we propose to partially close the knowledge gap in Scenario 1 by finding that delegate certificates are a viable method for originating providers to establish a verified association between a customer that is an initiating provider and the number being used to initiate the call, and we seek comment on this view. Delegate certificates, which are described in ATIS-1000092 (a separate ATIS standard than those required for STIR/SHAKEN implementation) allow an entity to obtain a certificate from the TNSP that demonstrates the entity's authority to use the number and present that certificate to the originating provider. We believe this process would enable initiating providers to satisfy this criterion whenever its end user customer uses a telephone number that the initiating provider assigned to the end user. To what extent are providers already using delegate certificates for this purpose? What measures, if any, are needed to ensure that delegate certificates are accepted as a valid form of showing an initiating provider has a relationship with a number? Must we require that originating providers accept delegate certificates from initiating providers as evidence they have a verified association with a number, and if so, should we place any guardrails on this requirement? What are the benefits and drawbacks of the delegate certificate approach? Because the delegate certificate would be associated with the TNSP, would it enable the TNSP to be held accountable for the illegal calls transmitted by entities to which they assigned numbers? Should we further find that delegate certificates are a viable method for originating providers to establish a verified association between an end user customer, such as a non-voice service provider enterprise, and the number being used to initiate the call? ~~If so, does the Governance Authority need to modify its SPC token policy so that such end users can obtain SPC tokens and certificates? What are the risks and benefits of allowing non-provider entities to have a role in the STIR/SHAKEN ecosystem?~~ We seek comment on any additional provider and customer arrangements for which delegate certificates could be used to establish a customer's association with a number.

Proposed Edit to Paragraph 12
(footnotes omitted)

12. Whether they actively collaborate with fraudsters, turn the other way when bad actors use their networks or services to transmit illegal calls or defraud consumers, or simply fail to implement policies and procedures to fulfill their regulatory obligations to stop such nefarious activity, voice service providers that evade or ignore our rules undermine trust in the voice network and the effectiveness of tools designed to combat illegal calls. Providers and other industry stakeholders have been well positioned to identify "bad actor providers" and take rapid action to address them. The Commission established a flexible KYUP requirement that both empowers and obligates providers to identify bad actor providers and keep them from getting illegal calls onto the U.S. voice network. Similarly, the STIR/SHAKEN Governance Authority was designed to maintain trust in the STIR/SHAKEN framework by setting policies and procedures that govern the assignment of digital certificates used by providers to authenticate calls within ~~which providers may be a part of~~ the voice ecosystem. Despite these mechanisms, many bad actor providers remain.

Proposed Edit to Paragraph 46

(footnotes omitted)

46. We likewise propose to require the Governance Authority to largely follow the KYUP requirements to vet Certification Authorities prior to their selection, and that these requirements should be applied to existing Certification Authorities. The Governance Authority has not published a written policy governing the selection of Certification Authorities. Rather, the Governance Authority has established a policy for governing the issuance of certificates that is consistent with the STIR/SHAKEN standards, which Certification Authorities must follow in order to be considered a "trusted" Certification Authority.[87] We are concerned that some Certification Authorities may not be following the certificate issuance policy and may be nefarious actors. While a robust Certification Authority removal process could address such concerns, we believe the Governance Authority should take steps to identify bad actors before they are selected as Certification Authorities. Accordingly, we propose to require the Governance Authority to follow all of the information collection and information verification requirements we propose above. We also propose to require that the Governance Authority adopt a policy to review this information and deny Certification Authority when there is a reasonable basis for believing the Certification Authority is unlikely to comply with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies. We seek comment on our proposals and associated analysis, including whether we should require greater or lesser due diligence obligations. Should we also require the Governance Authority to adjust the certificate issuance policy, such as by changing the ~~establishing~~ a maximum expiration timeline for STI certificates?

Proposed Edit to Paragraph 47

(footnotes omitted)

47. We also seek comment on whether we should require the Governance Authority to establish a conflict of interest policy governing Certification Authorities' relationships with voice service providers, including when they are also acting as voice service providers, and what that policy should entail. Although the Governance Authority has established a policy concerning conflicts as to a Certification Authority also serving as the Policy Administrator, it has not established a conflict-of-interest policy as to a Certification Authority also acting as a provider or having common ownership ~~a close relationship~~ with providers for which the Certification Authority issues certificates. We are concerned about such relationships because a Certification Authority may have incentive to issue certificates to providers to which they are related without following the certificate issuance policy. We seek comment on this assessment.

Proposed Edit to Paragraph 48

(footnotes omitted)

48. Policies for the revocation of SPC tokens and removal of Certification Authorities. We propose to require that the Governance Authority play an active role in obtaining information about providers misusing their SPC tokens and take action on any information it receives or obtains. Under the Governance Authority's existing SPC Token revocation policy, providers must sign an agreement that contains the terms for which tokens may be used, such as in compliance with the STIR/SHAKEN standards governing proper attestations. The policy further states that the Governance Authority may revoke SPC tokens upon indication that a provider is in breach of the agreement, and lays out other specified reasons for revocation. Additionally, the policy imposes a standardized process stakeholders must use to report potential SPC token misuse. ~~Despite well-known reports that providers are applying improper attestations to calls or otherwise failing to follow the STIR/SHAKEN standards, the Governance Authority has reported to Commission staff that it has only revoked SPC tokens for providers that have failed to pay required fees or failed to supply annual FCC Form 499 revenue data, which the Governance Authority uses to calculate fees~~. We believe the Governance Authority may be hindered in enforcing the SPC token policy by relying on an overly formal reporting process to obtain information. To address this, we propose to require that the Governance Authority establish formal information sharing arrangements with the Industry Traceback Group and call analytics providers to receive information about specific providers' practices. We also propose to require the Governance Authority to review and evaluate information it receives from any sources, even in the absence of formal reports. Should we require the Governance Authority to seek additional information about providers, modeled off of the KYUP monitoring requirements we propose to establish above? Should we require it to relax its reporting policy so that stakeholders can submit information informally or anonymously? We see comment on our proposals and any aspects of our analysis.

Proposed Edit to Paragraph 49

(footnotes omitted)

49. We propose to require that the Governance Authority also play a more active role in seeking, and taking action on, information it receives about Certification Authorities failing to follow its policies. As noted, the Governance Authority has established a policy governing the issuance of certificates by Certification Authorities. It has also established a policy for the suspension or removal of Certification Authorities that violate the policy, violate their agreement with the Governance Authority, or have been involved in a cybersecurity incident. Anecdotally, Commission staff has learned that certain Certification Authorities issue a disproportionate number of certificates that are being used by voice service providers applying improper attestations to their calls. ~~We believe this is indicative of Certification Authorities not following the Governance Authority's certificate issuance policy.~~ To our knowledge, the Governance Authority has not suspended or removed any Certification Authorities. We propose to require that the Governance Authority establish a process to accept information about Certification Authority practices from stakeholders, including a process to regularly obtain information from call analytics providers. We further propose to require that the Governance Authority initiate investigations into Certification Authorities with suspect practices, such as a high volume of illegal calls associated with their certificates, and remove Certification Authorities who are found to be violating the certificate policy or their agreement with the Governance Authority. We seek comment on whether we should require the Governance Authority to obtain other information about Certification Authority practices that would inform their oversight. We also seek comment whether the Governance Authority has established adequate steps providers must take when they were issued certificates from a Certification Authority that was subsequently removed.