Secure Telephone Identity Governance Authority

Policy Decision 006: CA Suspension and Revocation Policy

Draft Version 3.0
Adoption Date: 3/25/2026
Publication Date: 3/26/2026
Status: Published

This Policy Addresses Suspension and Revocation of STI-CA Authorization Due to Violations of the Certification Policy and Security Incidents and Other Violations of the Secure Telephone Identity Certification Authority Agreement

If an authorized Secure Telephone Identity Certification Authority (STI-CA) fails to fulfill its requirements to provide and keep updated its Corporate Identity and Reputational Information (CIRI) and other due diligence information, meet its obligations under the Certificate Policy (CP), violates the terms of its agreement with the STI Policy Administrator (STI-PA) (CA Agreement), and/or discovers a "cybersecurity incident" (as defined below), the following process will be followed. The process addresses all STI-CA violations and any "cybersecurity incidents," whether or not such incidents constitute violations of the CA Agreement.

Completion of the process in this policy, while mandatory, shall not be considered a remedy for any breach of the CA Agreement, except at the sole discretion of **the STI-GA**. This process does not limit any rights available to the **STI-GA** or other parties in the event of a breach of the STI-CA's obligations.

A "cybersecurity incident" is any determined or reasonably suspected (i) unauthorized access to or disclosure or acquisition of Certification Authority Data (as defined in the CA Agreement); or (ii) act or omission that materially compromises the security, confidentiality, or integrity of Certification Authority Data or the physical, technical, administrative, or organizational safeguards put in place to protect the security, confidentiality, availability, or integrity of Certification Authority Data.

Step 1. Event Identification. The first step is the proper identification of a violation of the CIRI or due diligence information requirements, CP or CA Agreement and/or a cybersecurity incident that could lead to an STI-CA suspension or revocation (collectively referred to as the "event").[1] Information regarding events may come from an STI Participant, the STI-PA, or even a regulatory or law enforcement agency and must be delivered directly to the STI-GA Director and STI-PA within 24 hours of discovery. As part of this identification, it should be

[1] Revocation means the permanent cancelation of an STI-CA's ability to offer certificate assignment services within the SHAKEN ecosystem. Suspension is any action that temporarily limits in any manner determined by the STI-GA Board, an STI-CA's ability to offer certificate assignment services within the SHAKEN ecosystem.

determined and reported to the STI-GA Director whether the event (i) involves a potential violation of the CIRI or due diligence information requirements, CA Agreement or CP and/or (ii) involves a cybersecurity incident. Steps 1-8 of this process should be completed within 24 hours of the discovery of the event, or as soon as practicable based on the circumstances of the event.

Step 2: Immediate Mitigation Actions. Upon discovery or notification of the event, the STI-PA must take reasonable steps to limit the event's impact and scope. This may include suspending an alleged violators' access to the STI Service (as defined in the CA Agreement). The STI-PA must document each of these steps.

Step 3. Initial Notice of the Event. The STI-PA will send an official notice to the STI-GA regarding the identified event outlining the steps taken and to be taken by the STI-PA to address the event, such as shutting down the STI-CA's account, or revoking STI Certificates that may have been improperly assigned.

Step 4. Investigation. In cooperation with the STI-GA, the STI-PA will be responsible for investigating the event. This investigation will begin immediately after the identification of the event. The STI-PA will help determine the proper scope of the investigation based on the type of event (e.g., cyber, contractual and/or policy violation), but the following will be used as a guide.

> ***For a cybersecurity incident***, whether or not potentially related to a violation of the CA Agreement or CP, a prompt and thorough investigation must be undertaken by the STI-PA, with appropriate cooperation of the STI-CA, to identify the nature and cause of the incident, the impact to sensitive data and systems, appropriate mitigation actions, and other information. At a minimum, the STI-PA's investigation must address:
>
> 1. **The nature of the cyber security incident**; this involves consideration of how data was accessed.
>   - Was it in physical or electronic form, and how was it transferred? It could be that the system was intentionally hacked or perhaps the data was released by accident.
>   - Was the cyber security incident properly and timely detected?
>   - What was the issue that allowed the data to be exposed?
> 2. **The data which has been accessed**; the STI-PA must ascertain what data has been released, specifically which data fields and for what STI Participants. The STI-PA must ascertain who may have obtained unauthorized access to the data as a result of this cyber security incident. Is it an unknown third party, a known third party that is not an STI Participant, an authorized STI participant, or even someone within the STI-PA? If the STI-PA does not know if anyone actually has unauthorized access to the data, the STI-PA should surmise who *might* be able to access it without authorization.

- Was data exfiltrated? What evidence exists to substantiate exfiltration or support and inference that no exfiltration occurred? What risks have been created by exfiltration of data?
- How many STI-Participants are affected?
- Did they access any non-public 499 data?
- Was this the work of an authorized user, an outside party, or someone within the STI-PA or its controlling company?

3. **The extent of the damage and the extent of the potential damage**; If it is not known what the unauthorized recipient of the information is planning to use the information for, determine what could happen with it should it get into the wrong hands, and what might this mean for your data subjects? Consideration of how much data has been released, and how many data subjects are affected will also indicate the severity of the cyber security incident.
   - Were the STI-PA systems altered, or damaged as a result of the cyber security incident?
   - What are the potential dangers of the data being exfiltrated and misused?
4. **Whether data can be retrieved.** The STI-PA should consider investigating whether any inappropriately accessed data has been downloaded and, if so, whether this data can be recalled. The STI-PA should attempt to trace the destination of the data and seek the physical return of the information.
5. **Whether steps should be taken to terminate access.** The STI-PA will also need to consider whether passwords, or log-in codes need to be changed. If the cyber security incident cannot be stopped via means of user suspension, or software patch, a hardware response may be necessary.
   - If data was accessed by a known party, reach out to party to begin working with them to determine reason for cyber security incident, what happened to data and their willingness to cooperate in clean-up.
   - If the STI-PA has been able to access and isolate the hardware used and data accessed in the cyber security incident.
   - Whether the recipient is a good faith actor willing to cooperate in retraining the affected data and addressing the cyber security incident.
   - Whether passwords or log-in codes should be changed.
   - Whether user suspension or a software patch may mitigate the cyber security incident.
   - Whether a hardware response may be necessary.

For a contractual and/or policy violation, a prompt and thorough investigation must be undertaken by the STI-GA with the assistance of the STI-PA and with appropriate cooperation of the STI-CA, to identify the nature and cause of the event, the impact to the overall SHAKEN ecosystem, appropriate mitigation actions, and other information. At a minimum, the STI-PA's investigation must address the following:

1. **The nature of the violation**;
   - Was it a violation of the CIRI requirements or due diligence information requirements, CA Agreement or the CP?
   - Which obligations were not met?
   - Over what period of time has the violation occurred?
   - How was the violation discovered?
   - Is the violation ongoing or has it been resolved?
2. **The extent of the damage and the extent of the potential damage to the SHAKEN ecosystem**;
   - How many STI-Participants were involved/affected?
   - Does/did this event cause improper attestation of calls?
3. **Whether steps should be taken to terminate access.** The STI-GA will consider whether an immediate suspension of STI-CA services is warranted or if STI-Certificates assigned by the STI-CA need to be revoked, considering:
   - Whether the STI Certificates were assigned to, or have been retained by, unauthorized service providers or Resp Orgs.
   - Whether the STI-CA is acting in good faith and is cooperating to remedy the situation.

Step 5: Mitigation Actions. Once the STI-GA and STI-PA are confident that information sufficient to understand the nature and scope of the violation or event, they should consider whether additional steps are needed to mitigate the impacts. For a cybersecurity incident, mitigation must include an evaluation of any STI-PA system vulnerabilities and the implementation of any needed system patches as soon as possible.

Step 6: Communications with the STI-CA. If the violation is of the CA Agreement, or a cybersecurity event is involved, as the holder of the CA Agreement, the STI-PA will handle all direct communications with the affected STI-CA. The STI-PA shall inform the STI-CA that all communications from the STI-CA about the alleged violation will go through the STI-PA and not directly to the STI-GA or the STI-GA Board. If the violation is of the CIRI or due diligence information requirements requirements, or CP, the STI-GA may choose to handle direct communications with the STI-CA, involving the STI-PA where necessary.

Step 7: Initial Investigation Report. The STI-PA should provide an initial report to the STI-GA on the details of the violation. This report should include as much detail as possible about what the STI-PA knows and does not know with regard to the violation and, specifically, which sections of the CA agreement may have been violated. Where a violation of the Certificate Policy may have occurred, a report must be generated by the STI-GA that identifies the specific sections of the CP may have been violated. Where a violation involves a failure to provide, or keep updated, the necessary CIRI or due diligence information, the STI-GA will identify the specific information that is missing, or out-of-date. These reports must be provided to the STI-GA Board.

Step 8: Industry Notifications. ATIS will draft for STI-GA Board approval any required notifications to external parties. This should be done as soon as possible and may need to be considered prior to the interim meeting. External party notifications may include:

- FCC
- Other Federal and State Agencies
- STI Participants (STI-CAs, SPs and Resp Orgs)

Timing is particularly important for cybersecurity incidents, whether or not related to a violation of the CA Agreement. Timely notice of a cybersecurity incident will allow STI-PA participants affected by the incident to change passwords, or cancel accounts, and otherwise mitigate the impact of the event.

Step 9: STI-GA Board Review to Discuss Event. A STI-GA Board interim meeting(s) will be held to share information about the event and any action taken by the STI-PA to date.

Step 10. STI-PA Recommendation. For a cybersecurity incident or CA Agreement violation, the STI-PA shall recommend, based on its analysis of the event, to the STI-GA what steps (if any) should be taken to resolve this matter. For a violation of the CP, the STI-GA shall receive a recommendation, based on an analysis of the event, regarding what actions (if any) should be taken to resolve this matter. Actions may include temporary or permanent suspension of the CA's access to the STI service, conditional reinstatement, or reinstatement without conditions. If conditional reinstatement is recommended, the report shall recommend conditions to the STI-GA Board. If the event is a cybersecurity incident, the STI-PA will also identify any necessary changes to STI-PA data handling/system protection that are necessary to prevent reoccurrence of the incident.

Step 11. Board Review of Recommendation. The STI-GA Board will consider the recommendation received and approve, reject or modify this recommendation. The STI-PA will be informed of the Board's decision on this matter.

Step 12. **STI-PA Review/Implementation of Recommendation.** The STI-GA Board's decision will be communicated to the STI-CA. Any reports provided by the STI-CA as part of a conditional reinstatement must be shared by the STI-PA with the STI-GA.

Step 13: Final Messaging. ATIS will draft for STI-GA Board approval a final event notification to any external parties that need to be notified. External party notifications will likely include, at a minimum, all entities to which the initial event notification was issued.

Step 14. Post Event Review. The STI-GA Board should convene to discuss all aspects of the event and consider any changes to the process followed in responding to it, including whether any changes should be considered to the STI processes, policies and/or contracts.

Step 15. Audit. If the investigation of this matter confirms that there was a violation of the CA Agreement or CP, a post-mortem should be done to consider how to improve the processes and prevent the recurrence of the violation.

A third-party assessment of the STI-CA's processes should also be considered to ensure that it has remedied any issues that led to the event.

For a cybersecurity incident, it should be considered whether a full security audit of the STI-PA systems is necessary to minimize the likelihood of recurrence. A third-party assessment of the STI-CA should also be considered to ensure that any improperly obtained data has been deleted.