

CHaaS and Recorder Performance Standards and Service Level Agreements

Service Level Agreement

An agreement between the State and the Respondent that specifies, in measurable terms, the services that the Respondent will furnish.

System Performance Standards and Reporting

Respondents must identify the SLAs and metrics for the system components that will be utilized to formulate the system performance measurements for each performance standard.

System Availability

The service must be available 99.999 percent of the time and is measured on a per-PSAP basis.

Service Level and Service Management Performance Standard

Services referenced here are limited to those provided under the agreement. All times are averages over a rolling 12-month measurement period. However, there are provisions for declaring an SLA violation in cases where repeated instances occur over a short period of time.

All time intervals are calculated to the nearest minute. Performance requirements are applicable to managed and non-managed services.

Regular Business Hours

Hours between 8:00 a.m. and 5:00 p.m. US Eastern time.

NOC/SOC Availability

Resources will be available (via toll-free telephone number) 24 x 7 x 365 to process requests for support.

Technician Availability

Onsite technicians will be available remotely and/or onsite as required, on a 24 x 7 x 365 basis.

Web-based Trouble Reporting and SLA Tracking

It is desirable that trouble reporting and SLA tracking are reported via a secure web-based portal.

CHaaS and Recorder Incident Severity Levels

Incident severity level definitions are consistent with those in Acceptance Testing. For the post-cutover environment, some examples are provided below of issues that would be classified according to the specified severity.

Severity Level 1 – Critical

An incident shall be categorized as “Severity Level 1” if it renders a critical system, service, software, equipment, or network component unavailable or substantially unavailable, or seriously impacts normal business operations; in each case, prohibiting the ability to process a request for assistance for one or more PSAPs, or a single individual performing a critical function. Examples of conditions may include:

- Isolation of any single site or sites from the rest of the network, resulting in the inability for affected sites to communicate with the rest of the network.
- A software defect without a workaround that impacts any site's or sites' ability to maintain business operations.
- A reduction in call-handling or recording capacity at a single site of 50 percent or more.
- Cybersecurity attack detected to be in progress or highly likely/imminent.
- Faults affecting critical 9-1-1 service resulting in:
 - The inability for a caller to connect through voice dialing or texting with a PSAP.
 - The inability for a PSAP to receive audio with an emergency call, (when audio is expected).
 - The inability for a PSAP to receive location information with a 9-1-1 call.
 - The inability for a PSAP to receive callback information with a 9-1-1 call.
 - The inability for a PSAP to have their 9-1-1 calls recorded.

Severity Level 2 – Major

An incident shall be categorized as “Severity Level 2” if the incident does not render a critical system, service, software, equipment, or network component unavailable or substantially unavailable, but a function or functions are not available, substantially available, or functioning as they should; in each case, impacting the ability to process a request for assistance for one or more PSAPs, or a single individual performing a critical business function. Examples of conditions may include:

- Loss of network or redundancy, including a CHaaS or recording node or PSAP connectivity.
- System or component problem that could result in a PSAP outage without timely repair.
- A reduction in system capacity at a PSAP of 20 percent or more.
- Inability for CHaaS to accurately display critical information like callback number or location information.

Severity Level 3 – Minor

An incident shall be categorized as “Severity Level 3” if the incident causes a group or individual to experience trouble accessing or using a system, service, software, equipment, or network component, or a key feature thereof, and a reasonable workaround is not available, but does not prohibit the execution of productive work. Examples of these conditions may include:

- Inability for certain users or roles to access management dashboards/portals or run reports.
- Failure of a common function like monitoring, requiring manual intervention or other additional steps to achieve the desired result.

Severity Level 4 – Non-Service-Impacting

An event shall be categorized as “Severity Level 4” if the incident impacts a PSAP, a group, or individual with minor usability problems but does not prevent or hinder functionality. Examples of these conditions may include:

- Errors in data display/presentation with an application.
- Errors with peripheral systems such as workstation equipment, tools, or applications.
- Errors with monitoring systems, dashboards, etc.
- Items committed to by the Respondent that are planned for future release (software development)

Response Time

A qualified resource acknowledges requests for assistance by the State or PSAP via phone or email and commences investigation of trouble within the timeframes identified in the table below.

Table 1: Response Time

Trouble Category	Response Time
Severity Level 1	15 minutes
Severity Level 2	30 minutes
Severity Level 3	8 hours
Severity Level 4	12 hours

Notification Time

The time from when an issue is identified and the State or PSAP is informed of the issue. Contractor shall have the ability to provide customized notifications based on desire of the State or PSAP.

Table 2: Notification Time

Trouble Category	Notification Time
Severity Level 1	15 minutes
Severity Level 2	30 minutes

Severity Level 3	8 hours
Severity Level 4	Next Business Day

Repair Time

Issues documented via the ticketing process will be resolved in the timeframes identified in the table below. Resolution may be either the final repair that returns the system to its normal functioning condition, or a PSAP-accepted workaround accompanied by a plan to achieve the final repair.

Table 3: Repair Time

Trouble Category	Interval
Severity Level 1	2 hours
Severity Level 2	4 hours
Severity Level 3	48 hours
Severity Level 4	96 hours

Escalation

In cases where an interval identified in the table below has elapsed from the time the ticket was created, a request for assistance to the next higher level of technical support must be executed.

Table 4: Escalation Intervals

Trouble Category	Interval
Severity Level 1	2 hours
Severity Level 2	4 hours
Severity Level 3	48 hours
Severity Level 4	96 hours

Once an escalation has occurred, Contractor will provide the State and affected parties with a status update within the agreed-upon interval until resolution.

CHaaS IP Network Measurement and Reporting Requirements

Network Performance

The selected Respondent must measure and report on the network performance against the service levels monthly. For any network downtime, outages, or interruptions, the selected Respondent must provide a written report describing the degradation of service or outage, including the root cause and the plan to prevent similar occurrences in the future. Trend data must be supplied with this report that shows current and previous monthly performances.

Service Interruption and Outage Reporting

As defined in 47 CFR § 4.5, the Respondent is responsible for complying with all federal reporting requirements for any outages or interruptions to 9-1-1 voice or SMS text delivery, and/or processing systems and services provided under a contract. The Respondent is required to electronically report significant network outages and information about outages that

exceed specific thresholds—in terms of duration and magnitude—to the FCC's Network Outage Reporting System (NORS). The electronic report shall also include information regarding communications disruptions affecting any 9-1-1 facilities.

Root Cause Analysis Reporting

In the event of an unplanned service interruption or outage that results in a Severity 1 or 2 incident or in an SLA being missed, the Contractor must provide the State with a Root Cause Analysis (RCA) report. An initial written explanation of the problem and the planned resolution will be provided by the vendor within 5 business days, with a final report provided within 30 calendar days, measured from the beginning of the service affecting issue. This report will include the timeline and duration of the interruption/outage, the cause of the interruption/outage, the corrective actions taken to resolve the interruption/outage, and any actions/processes undertaken by the Respondent and its subcontractors to prevent similar issues from occurring in the future, or to mitigate their impact, if they do.

Bandwidth Management

The Respondent shall provide monthly bandwidth performance and network utilization reports.

State must be able to monitor overall bandwidth usage and specific usage between sites. State must be able to view real-time or near-real-time bandwidth performance and utilization reports. Users of the monitoring tools should be able to filter on various traffic characteristics (e.g., protocol, QoS classification, media type, etc.). A web-based portal or browser-enabled viewer is required.

The Respondent's call-processing capacity shall be capable of 125% busy hour call traffic for the PSAP.

The Respondent's service shall be able to increase call-processing capability by up to 50% over contract duration with no critical hardware upgrades required.

Voice Quality and Quality of Service

Voice quality must be maintained at traditional Public Switched Telephone Network (PSTN) levels. Voice data (RTP¹) must have priority over any other IP traffic and this priority must be respected and enforced by all network infrastructure elements, end-to-end. The service shall use an uncompressed, high quality voice codec. The CHaaS must not degrade the Mean Opinion Score (MOS) of calls traversing its network by more than two-tenths (0.2) and must maintain a Mean Opinion Score (MOS) standard rating of 4.0 or higher.

Network Management and Monitoring

The Respondent must provide a NOC/SOC to respond to network issues and meet the service levels stated within this document, including requirements for a secondary or backup NOC, and monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems to identify anomalous activity that could be indicative of a security incident or compromise.

Proactive Monitoring

The Respondent must provide active monitoring of its Service as a whole, including; network, replication, hardware, software, call processing, etc. The Respondent must proactively generate incident tickets and alert the State and affected PSAPs in accordance with the incident severity level tables above regarding Response or Notification Times.

CHaaS SLA Reporting

A secure online SLA reporting dashboard is required. The SLA reporting dashboard shall include both real-time and/or near real-time performance data captures in no greater than five-minute averages. The SLA reporting tool shall

¹ Real-time Transport Protocol

summarize network performance metrics by hour, day, week, month, quarter, and year. The mechanism shall deliver automated SLA results to State on a monthly and quarterly schedule. (The quarterly results are simply an aggregation of the monthly reports).

Quality of service (QoS) reporting shall present traffic by type. Reports shall include, at a minimum, statistics for latency, jitter, packet loss, and bandwidth utilization, and shall be available on demand with near real-time data. Other relevant data also may be reported.

Contractor shall conduct end-of-month and end-of-quarter service reviews, accounting for any degradation of service to include service failures, as well as incidents and problems, and their resolution.

SLA remedies shall be credited to their full amount, but the maximum credit per month shall not exceed 25 percent of the total monthly service fee.

Incidents shall be tracked via support tickets and the ticket contents shall be made available to the State and PSAPs. Contractor shall have automated systems to track all SLA deliverables and provide the State with monthly reports detailing Contractor performance.

The monthly SLA compliance report shall include the following detail and a one-page summary for every Severity 1 and 2 problem that occurred during the month:

- 1) Report period;
- 2) Contractor's trouble ticket number;
- 3) Name(s) of affected PSAP(s);
- 4) FCC IDs of affected PSAP(s);
- 5) Service type;
- 6) Brief trouble symptom;
- 7) Brief restoration description;
- 8) Trouble symptom category;
- 9) Ticket open date and time;
- 10) Severity level;
- 11) Problem resolution date and time;
- 12) Total duration;
- 13) Yes/no if qualified for SLA;
- 14) Yes/no if FCC reporting required;
 - i. If yes, link to FCC report and FCC response, if any
- 15) The applicable SLA; and
- 16) Rights and remedies applied to each ticket when applicable.

Table 5: CHaaS SLA Violations, Damages, and Requirements

SLA	Definition	Measurement Method	Objective	Rights and Remedies
1	Final master project plan (MPP) shall be delivered to the State within sixty (60) calendar days of contract execution.	Calendar Days	Delivery of MPP within 60 days.	Failure to meet the objective shall result in a \$5,000.00 credit/or adjustment for each calendar day that the report is not delivered after the objective date.
2	Contractor shall achieve all milestone dates identified in the MPP.	Calendar Days	Completion of MPP milestones within the date agreed by the State and Contractor.	Any failure to meet the objective shall result in a \$5,000.00 credit/or adjustment for each calendar day that the milestone is not delivered after the objective date (for milestones with a majority of the underlying task ownership being that of the Contractor and/or its subcontractors).
3	SLA Remedy Delivery: Timely credit/or adjustment of remedies due to the State for missed SLA objectives.	Calendar Days	Contractor's credit/or adjustment shall be issued no more than sixty (60) calendar days after written notice of the violation from the State.	Each occurrence of an SLA remedy (credit/or adjustment) that is not issued within sixty (60) calendar days shall result in a \$5,000.00 credit/or adjustment for each calendar day that the credit/or adjustment is not issued.
4	Contractor shall provide a ticketing interface and monitoring dashboard 24 hours a day, 7 days a week, 365 days a year (24 x 7 x 365)	The monthly availability percentage equals the Scheduled Uptime less Unavailable Time divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is based on 24 hours x number of days in the month x 60 minutes. The monthly Availability percentage shall be based on the cumulative total of all outage durations for each calendar month.	99.9% (8.77 hours per year 43.83 minutes per month)	Failure to meet the SLA objective for one month shall result in a \$2,500 credit/or adjustment of the total Monthly Recurring Charge (MRC) of all services under contract for that month.

SLA	Definition	Measurement Method	Objective	Rights and Remedies
5	Contractor shall report all outages and service interruptions that potentially impact the delivery of 911 traffic (voice, ANI, ALI) to every affected PSAP within 15 minutes of the occurrence.	Any outage or service interruption that potentially impacts the delivery of 911 traffic, regardless of traffic type	Notification within 15 minutes or less.	Any failure to meet the objective shall result in a \$5,000.00 credit/or adjustment Every next consecutive minute that the Contractor fails to meet the SLA objective shall result in an additional \$1,000.00 credit/or adjustment per minute, up to the total MRC for all services.
6	Failure to provide updates to solution to conform to NENA i3 standards within 18 months of ratification.	Identification by the State or its designee of i3 functionality not supported.	100% conformance to NENA i3 standards within 18 months of ratification.	20% credit/or adjustment of total monthly invoice until conformance issue is resolved to State's satisfaction.
7	The CHaaS network must transport voice calls with little or no degradation of voice quality, as measured and monitored by an automated Mean Opinion Score (MOS) measurement tool.	The CHaaS network shall be defined as the IP network between the CHaaS hosts and the PSAPs, as well as the IP network between CHaaS hosts.	99% of the MOS measurements shall not degrade by more than 0.2 from the ESInet demarcation point at the CHaaS host sites to the PSAP workstations (e.g., an MOS of 4.0 shall not degrade lower than 3.8)	\$5,000 credit/or adjustment of MRC of CHaaS for single occurrence. \$10,000 credit/or adjustment of MRC of CHaaS for second occurrence with a 60-minute period.
8	The CHaaS will receive and handle all call type traffic with minimal service interruption.	Single outage with a duration of six (6) minutes or more.	Preventing outages of six (6) minutes or more.	100% credit/or adjustment of the MRC of CHaaS for the affected PSAPs.
9	The CHaaS will receive and handle all call type traffic with minimal service interruption.	Single outage of greater than two (2) minutes and less than six (6) minutes.	Preventing outages greater than two (2) minutes, but less than six (6) minutes.	50% credit/or adjustment of the MRC of CHaaS for the affected PSAPs.
10	The Contractor shall provide the CHaaS SLA reporting required by this contract for each month of activity during the term of the contract by the 10 th business day of the following month.	Business Days	The Contractor shall deliver accurate and complete reporting by the 10 th calendar date of the month following the end of the applicable reporting month.	Failure to meet the objective shall result in a \$5,000.00 credit or adjustment for each business day that the reporting is not delivered after the objective date.

SLA	Definition	Measurement Method	Objective	Rights and Remedies
11	Contractor shall provide a cybersecurity vulnerability notification upon recognition of a cybersecurity threat or breach within three (3) business days of issue identification.	Business Days	Within three (3) business days of the recognition of a vulnerability or identified cybersecurity threat or breach, the Contractor shall notify the State and the impacted PSAP(s) of the event, and measures taken to mitigate impact and avoid future risk.	Failure to meet the objective shall result in a \$5,000.00 credit or adjustment for each business day that the report is not delivered after the objective date.
12	Contractor shall provide a Root Cause Analysis (RCA) report for Severity Level 1 and 2 issues within five (5) business days.	Business Days	The Contractor shall deliver initial root cause analysis to the State and the affected PSAPs within five (5) business days of service affecting issue.	Each occurrence of a failure to meet the objective shall result in a \$15,000.00 creditor adjustment for each business day that the report is not delivered after the objective date.
13	Contractor shall provide a final RCA report within thirty (30) calendar days from the beginning of the service affecting issue.	Calendar Days	The Contractor shall deliver final RCA to the State and the affected PSAPs within thirty (30) calendar days from the beginning of the service affecting issue.	Each occurrence of a failure to meet the objective shall result in a \$15,000.00 credit/or adjustment for each business day that the report is not delivered after the objective date.