Attachment C – ESInet/NGCS Performance Standards, Network Measurements and Reporting, and Service Level Agreements

1. Performance Standards and Terms

A. Service Level Agreement (SLA)

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

B. Help Desk Availability

The time-of-day resources are available to answer calls from GCRECD, create trouble tickets, and dispatch technicians.

C. Access to Technical Staff

The time-of-day technicians are available to assist GCRECD remotely and/or onsite.

D. Regular Business Hours (RBH)

Hours between 8:00 a.m. and 5:00 p.m. Central.

E. Response Time

The interval between a trouble ticket being created and when a qualified resource is actively involved in addressing issues recorded in a trouble ticket.

F. Repair Time

The interval between a trouble ticket being created and the technology issue is resolved, or an acceptable workaround is in place, and all functions have been restored to normal**.**

G. 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.

H. System Availability

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

I. 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 apply to managed and non-managed services.

J. Help Desk Availability

Resources will be available (via an agreed-upon telephone number) 24 x 7 to process requests for service.

K. Technician Availability

Technicians will be available remotely and/or onsite as required 24 x 7.

L. Web-Based Trouble Reporting and Tracking

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

M. Incident Severity Levels

1) Severity Level 1 – Critical

An incident shall be categorized as a "Severity Level 1" incident if the incident is characterized by the following attributes: the incident (a) renders a business-critical system, service, software, equipment, or network component unavailable or substantially unavailable, or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function. Examples of conditions may include:

- Isolation of any single site or sites from the rest of the network, resulting in the inability of affected sites to communicate with the rest of the network
- Loss of any single circuit
- Decrease in throughput equal to or greater than 20 percent of capacities at any data center

2) Severity Level 2 – Major

An incident shall be categorized as a "Severity Level 2" incident if the incident is characterized by the following attributes: the incident (a) does not render a business-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 prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function. Examples of conditions may include:

- Loss of redundancy at data center connections
- System or component problem that could result in loss of a site without timely repair
- Decrease in throughput equal to or greater than 20 percent on any one circuit

3) Severity Level 3 – Minor

An incident shall be categorized as a "Severity Level 3" incident if the incident is characterized by the following attributes: the incident causes a group or individual to experience an incident with 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.

4) Severity Level 4 – Maintenance

An event shall be categorized as a "Severity Level 4" incident if the incident is characterized by the following attributes: the incident impacts a group or individual affected by planned maintenance of the "service" or non-service impacting incident.

N. Response Time

A qualified resource acknowledges requests for assistance by GCRECD or via phone or email and commences an 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	Next Business Day
Severity Level 4	Next Business Day

O. 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 GCRECD-accepted workaround accompanied by a plan to achieve the final repair.

Table 2: Repair Time

Trouble Category	Repair Time
Severity Level 1	2 hours
Severity Level 2	4 hours
Severity Level 3	48 hours
Severity Level 4	5 business days

P. Escalation

Escalation of problems is critical to the quality of service provided. 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 3: Escalation Intervals

Trouble Category	Interval
Severity Level 1	30 minutes
Severity Level 2	1 hour
Severity Level 3	36 hours
Severity Level 4	96 hours

Once an escalation has occurred, the Respondent will provide GCRECD with a status update within one-half of the escalation interval based upon the severity level, and then every 72 hours until a resolution path is agreed upon.

2. IP Network Measurements and Reporting

A. Network Performance

The selected Respondent must measure and report on the network performance against the service levels monthly. For any circuit 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.

B. Outage Reporting

In the event of an unplanned outage, the selected Respondent must provide GCRECD a reason for outage (RFO) report. This report will include the timeline, the cause of the outage, actions taken to resolve the issue, and any actions/processes to prevent similar outages from occurring in the future. GCRECD requires a preliminary report within 72 hours of the event and a final report within 10 business days, to be measured upon correction of the outage.

C. Bandwidth Management

GCRECD must be able to observe overall bandwidth usage and specific usage between sites. The selected Respondent's solution must be able to create detailed SLA monitoring reports in real-time. GCRECD must be able to view real-time or near-real-time bandwidth performance and utilization reports. The solution should automatically determine the traffic type and provide various views into bandwidth usage. A web-based portal or browser-enabled viewer is preferred.

D. Voice Quality and Quality of Service (QoS)

Voice quality must be maintained at traditional public switched telephone network (PSTN) levels and have priority over any other Internet Protocol (IP) traffic. The solutions in place today use the G.711 codec, and the network must support voice quality that meets or exceeds ITU-T-P.830 and must be able to maintain a Mean Opinion Score (MOS) standard rating of 4.0 or higher.

E. Network Management and Monitoring

The selected Respondent must staff a network operations center (NOC) to respond to network issues and meet the service levels stated within this RFP.

F. Proactive Monitoring

The selected Respondent must provide active monitoring of its circuits for all network performance indicators described in Section 3.4 of the RFP. The selected Respondent must proactively generate incident tickets and alert GCRECD (defined in incident severity level tables above) for response times.

3. Service Level Agreement

An SLA is a contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service.

A. SLA Reporting

Respondents shall describe their reporting tool. A secure online SLA reporting tool is preferred. SLA reporting tools are expected to include both real-time and/or near real-time performance data captures in no greater than five-minute averages. The SLA reporting tool shall summarize network performance metrics by the hour, day, week, month, quarter, and year. The mechanism must deliver automated SLA results to GCRECD monthly. 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. A web-based portal is preferred. Other relevant data also may be reported.

Respondents shall specify how they will conduct and provide end-of-month and end-of-quarter reviews, accounting for any degradation of service including service failures, as well as incidents and problems, and their resolution.

Incidents shall be tracked via tickets and the ticket contents shall be made available to GCRECD.

The network provider shall have automated systems to track all SLA deliverables and provide GCRECD with monthly reports detailing the provider's performance.

B. SLA Violations

An SLA violation shall have occurred whenever the selected Respondent fails to meet any single performance level.

An SLA violation shall have occurred whenever the average of any single performance item over the preceding two-month period fails to meet the service level. This is an "early warning" of an unacceptable trend.

C. SLA Violation Damages

Damages shall apply whenever:

- Any single-performance-item SLA violation occurs in two consecutive months.
- Any single-performance-item SLA violation occurs the month following an occurrence of an "early warning" SLA violation per the section titled SLA Violations of this document.
- Any single SLA violation as described in Appendix B, paragraph 1, section M 1), Incident Severity Levels, occurs for more than four hours.

A chronic service outage will be deemed to have occurred if GCRECD experiences more than six outage occurrences, as identified in Appendix B, paragraph 1, section M 1), Incident Severity Levels, in a rolling 12-month period, or if a service outage occurs for more than 24 hours and is not the fault or negligence of GCRECD.

D. SLA Specific Network Service Requirements

1. Network Availability >/= 99.999 percent
2. Latency </=50 ms
3. Packet Delivery >/=99.9 percent
4. Jitter </= 5ms latency one-way, end-to-end
5. Less than 0.1 percent packet loss
6. Granular web-based QoS controls not limited to percentage allocations
7. Proactive circuit monitoring and 5-minute proactive notification for circuit outage
8. Real-time customizable packet-filtering portal
9. Packet analytics storage for all packets for 90 days
10. Accept and honor QoS markings (i.e., Differentiated Service Code Points [DSCP]) as presented by GCRECD equipment, and pass markings through the network unmodified

E. Installation

Less than 60 business days or 12 calendar weeks for each circuit to be installed and ready for turn-up. Anything greater than 60 days will equate to one day's credit per circuit not delivered, applied to the first month's bill.