



METROPOLITAN EMERGENCY SERVICES BOARD 9-1-1 TECHNICAL OPERATIONS COMMITTEE AGENDA

September 19, 2024 10:00 a.m.

1. **Call to Order & Introductions** - Susan Bowler, 2024 Committee Chair Susan Bowler
2. **Approval of Agenda** - Bowler
3. **Approval of Minutes** – August 15, 2024 Meeting - Bowler
4. **Action Items**
 - A. None
5. **Discussion Items**
 - A. Presentation/Discussion: SAFECOM Nationwide Survey – Devin Christensen CISA
 - B. Mapped ALI Solution Offerings – Heidi Hieserich
 - C. Mental Health Call Processing Standard - Tony Martin
 - D. MESB 2022-2024 Interoperable Emergency Communications Strategic Plan (IECSP) - Jacobson
 - E. ECN Update/Status – ECN
6. **Reports**
 - A. PSAP Operations Roundtable Workgroup - Heidi Meyer
 - B. SECB NG9-1-1 Committee Report - Janelle Harris/Brent Anderson
 - C. 9-1-1 GIS and Data Report (attached) - Marcia Broman
 - D. 9-1-1 Network Report (attached) - Jacobson
 - E. MN Sheriff's Assoc. PSAP Subcommittee Report - Bowler
 - F. IPAWS Report - Kari Morrissey
 - G. SECB NG9-1-1 Technical Operations Workgroup - Scott Petersen
 - H. SECB NG9-1-1 Operations Workgroup - Morrissey
7. **New Business - None**
8. **Announcements/Roundtable**
 - A. Roundtable: Each PSAP to share at least one item
 - B. Next Meeting: October 17, 2024, 10:00 am.
9. **Adjourn** – Bowler

**Metropolitan Emergency Services Board
9-1-1 Technical Operations Committee
Meeting Minutes
August 15, 2024**

Committee Members Attendance:

Airport – Sara Boucher-Jackson
Allina EMS – Victoria Vadnais
Anoka County – Kari Morrissey
Bloomington – **absent**
Carver County – Susan Bowler
Chisago County – Mike Parker
Dakota County – Heidi Hieserich
Eden Prairie – Lisa Vik
Edina – Janelle Harris
Hennepin County – Tony Martin
Hennepin EMS – **absent**
Isanti County – Robert Shogren

M Health EMS – Elias Charif
Metro Transit – Chad Ladda
Minneapolis ECC– Joni Hodne
North Memorial – **absent**
Ramsey ECC – Nancie Pass
Ridgeview EMS – John Scheuch
Scott County – Carrie Bauer
Sherburne County – Laura Anderson
St. Louis Park – Eric Lammle
U of M – **absent**
Washington County – Dar Pankonie

Alternates/Guests: Bobby Adney, *Hennepin County*; Brent Anderson, *Dakota County*; Marvin Bachmeier, *HCMC*; Jill Bondhus, *ECN*; Chad Gappa, *Motorola*; Heidi Meyer, *ACECC*; Scott Petersen, *Minneapolis ECC*; Steve Tait, *ECN*; and Dave Taylor, *IES*.

MESB Staff: Marcia Broman; Jake Jacobson; Jacob Kallenbach; and Jill Rohret.

1. Call to Order

Susan Bowler called the meeting to order at 10:00 a.m.

2. Approval of Agenda

Agenda item 5A was moved to 10A. Agenda item '4E: Mapped ALI RFP Awarding' was added to the agenda. Sections 4 and 5 were switched in order and will assume their new order.

Motion made by Tony Martin, seconded by Vikki Vadnais to approve the August 2024 9-1-1 TOC meeting agenda with the mentioned changes. Motion carried.

3. Approval of Minutes

Dar Pankonie stated that there is a typo in section 8E for the spelling of "Martin".

Motion made by Martin, seconded by Joni Hodne to approve the June 2024 9-1-1 TOC meeting minutes with the mentioned changes. Motion carried.

4. Discussion Items

A. Updating MN Statewide Communication Interoperability Plan

Jake Jacobson states he will continue to work on the updating of the regionwide SCIP plans. He will attempt to bring the IOC workgroup together prior to one of the upcoming meetings to garner feedback on the work being done.

Nancie Pass stated that SCIP is usually done through the SECB and asked for clarification on these SCIP procedures.

Jill Rohret responded by stating that this SCIP plan is purely for regional purposes. The MESB is taking information from County SCIP plans from the previous year and using it to create a regional document.

MESB staff will continue to review, edit, update, and move forward in producing SCIP.

B. Blue Ethos Training

Jacobson states that he continues to work with Blue Ethos on the grant funded resiliency training. The goal is to have training occur in the late fall of 2024 with sessions occurring at PSAPs throughout the region. The contract is signed, and the scheduling process has begun.

Pass asked how long the individual training sessions are and how long they will go once beginning in the fall.

Jacobson responded by saying that the individual training sessions will last around four hours. Training will be completed by May 2025.

Pass stated that two training sessions will not be enough for Ramsey and that scheduling dates sooner is more optimal for PSAPs as additional planning on their end will be needed.

Bowler stated that PSAPs can share training sessions with other PSAPs in an attempt to ensure regionwide training availability.

C. Mental Health Call Processing Standard

Martin stated that they continue to wait for the final version of the dictionary of terms. There is 988/911 mental health training for dispatch staff in the works. The group will continue to do important work with mental health.

D. ECN Update/Status

Jill Bondhus stated that ECN continues to work on data collection for the 9-1-1 project. Please submit your worksheet if you have not yet submitted. There will be a cybersecurity second round offering for participation. Please reach out if you are interested. Steve Tait thanked Marcia Broman for her work with GIS and the help she provided to greater Minnesota.

Martin asked if there were any updates on position vacancies.

Tait responded by stating they are getting close to posting the position opening for the Director vacancy. The 9-1-1 Manager hiring process will begin when the new Director has been chosen.

Vadnais asked how NG911 funding possibilities will work for secondary PSAPs given configuration of CHS-1 in which primary PSAPs are members and will expect funding though secondary PSAPs will not.

Tait responded by stating the he will bring that question to the State and get an explanation.

E. Mapped ALI RFP Awarding

Martin stated that two contracts have been awarded for the Mapped ALI RFP and that both companies have begun reaching out to PSAPs to provide presentations. He would like to see a regionwide decision when it comes to choosing companies as opposed to having each PSAP decide on their own. A regional decision can help with metro wide data sharing efforts and overall interoperability.

Bowler stated that it would be advantageous to have both as operationally, things come in through both. Both companies have benefits, and both are missing certain areas.

Martin responded by asking if the State would provide both. If you don't choose one, could you still get access to the other? Do PSAPs need to add all data into both? Which should be the priority for a data sharing platform.

Pankonie stated that they need to see demos. This is a high priority for the Metro, and they need to know all the details to get this decision moving forward.

Rohret stated that clarification on costs and what the State will cover is needed. ECN needs to provide complete information and relay that communication to the PSAPs.

Martin stated that it would be ideal to bring both companies into a 9-1-1 TOC meeting to see hands on demos of various thought out scenarios.

Tait stated that he will send more detailed information to Jacobson and that he can then relay that information to the PSAPs.

Bondhus stated that you can return to the "free" version of the competing software version if taking the others premium. It is feasible to have access to both.

Jacobson stated that he will attempt to get both companies to provide demos at the next 9-1-1 TOC meeting.

5. Action Items

A. MESB Mapped ALI Representative for SECB Workgroup

Pass stated that they are asking for a volunteer from the region with operational and technical experience to participate in the workgroup.

Heidi Hieserich asked about the States timeline for the group.

Tait responded that the workgroup will likely be assembled in October/November.

Motion made by Pankonie, seconded by Martin to nominate Heidi Hieserich as the representative to the Mapped ALI workgroup. Motion carried.

6. Reports

A. PSAP Operations Roundtable Workgroup

Heidi Meyer stated that they are revitalizing the CTL roundtable and working on various metro related items.

B. SECB NG9-1-1 Committee Report

The committee worked on PST training and education opportunities, policy and bylaw review, and SECB standard development.

C. 9-1-1 GIS and Data Report

The report is available in the meeting packet.

D. 9-1-1 Network Report

The report is available in the meeting packet.

E. MN Sheriff's Association PSAP Subcommittee Report

The subcommittee talked about the Motorola contract and worked on updating various standards.

F. IPAWS Report

IPAWS is working on enabling wireless emergency alerts to streaming services.

G. SECB NG9-1-1 Technical Operations Workgroup

No meeting took place this month.

H. SECB NG9-1-1 Operations Workgroup

No meeting took place this month.

7. New Business – None

8. Announcements/Roundtable

A. Roundtable

Each PSAP shared an item that they are currently working on.

B. Next Meeting: September 19, 2024. 10:00 a.m.

C. PSAP Network Option Review

Discussion on this subject is pushed to a future meeting as time runs out.

9. Adjourn

The meeting was adjourned at 11:49 a.m.

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SAFECOM NATIONWIDE SURVEY

*STRENGTHENING EMERGENCY COMMUNICATIONS
WITH STRATEGIC TEAMBUILDING*

SEPT 19, 2024



Devin Christensen
September 19, 2024

1

Agenda

1. What is the SAFECOM Nationwide Survey?
2. How to improve SNS survey and distribution?
3. How the SNS team can support the MESB?



Devin Christensen
September 19, 2024

What is the SNS?

A data collection effort that helps CISA assess national emergency communications capabilities and identify and close gaps.



SAFECOM
**NATIONWIDE
SURVEY**

Devin Christensen
September 19, 2024

SNS Data Supports CISA's Mission

Data-driven decision making

Tailored programs and services

Awareness of capabilities
and gaps



SAFECOM
**NATIONWIDE
SURVEY**

Stronger Together

Persistent challenges require collaborative solutions

There is an adversary infiltrating our critical infrastructure



SAFECOM
**NATIONWIDE
SURVEY**

Devin Christensen
September 19, 2024

5

Survey Design Challenges

- Large, complex nation with diverse organizations and missions
- Seeking input on
 - Question design,
 - Survey distribution, and
 - Data products

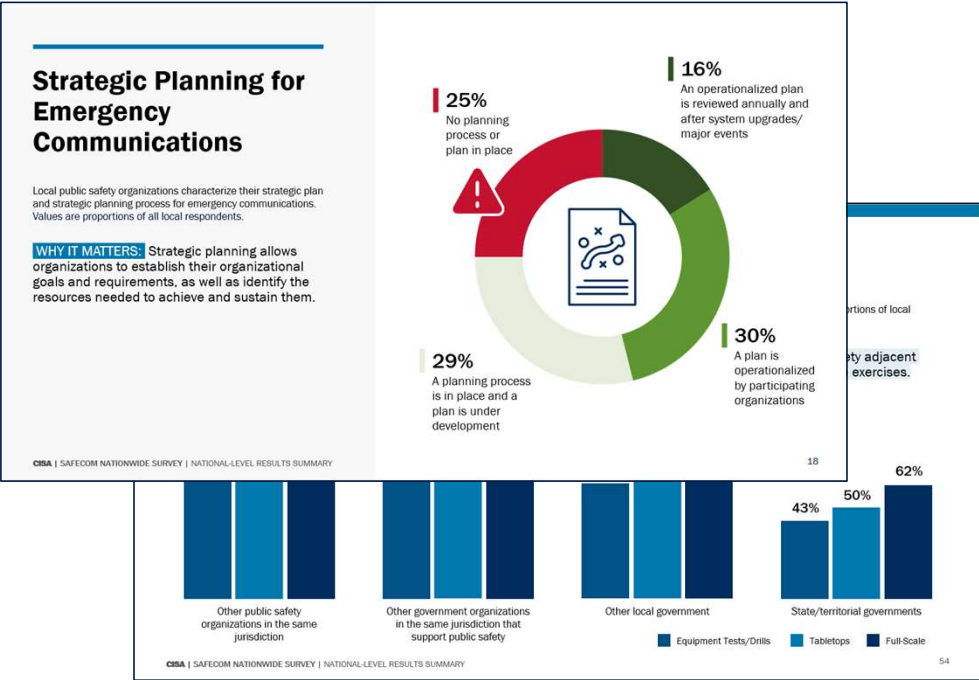
65,000
public safety
organizations
nationwide



SAFECOM
**NATIONWIDE
SURVEY**

Devin Christensen
September 19, 2024

Example Data Products



Q05_6) Select the responses that best characterize the agreements your organization has made to enable emergency communications interoperability with tribal governments/organizations. (SOR) Note: Reading from top to bottom, the first four responses are progressive (i.e., to select the fourth response, an organization must have surpassed all of the first three response criteria)

Answer Option	Discipline	All	Rural	Urban	Metro
There are informal, undocumented agreements in practice with	ALL	0.0772	0.0902	0.0843	0.0532
	ECC	0.0844	0.0951	0.0845	0.0728
	EM	0.0949	0.0984	0.1181	0.0625
	EMS	0.0897	0.1126	0.0921	0.0596
	FIRE	0.0845	0.0963	0.0946	0.0575
There are published and active agreements with some	LE	0.0683	0.0809	0.0645	0.0609
	ALL	0.0323	0.0379	0.0295	0.0293
	ECC	0.0336	0.0399	0.0366	0.0232
	EM	0.0408	0.0518	0.0302	0.0395
	EMS	0.033	0.0345	0.0385	0.0244
There are published and active agreements with most	FIRE	0.0284	0.0321	0.0264	0.0267
	LE	0.029	0.0392	0.0262	0.0226
	ALL	0.0351	0.0379	0.0309	0.0373
	ECC	0.0407	0.0307	0.0423	0.0487
	EM	0.0427	0.0492	0.0275	0.0526
Agreements are reviewed every 3-5 years, after system upgrades, or incidents that test capabilities with	EMS	0.0299	0.0276	0.0214	0.0434
	FIRE	0.0348	0.0374	0.0295	0.039
	LE	0.0423	0.0515	0.0363	0.0406
	ALL	0.0178	0.0159	0.0169	0.0213
	ECC	0.0132	0.0184	0.0113	0.0099
Not applicable	EM	0.0256	0.0207	0.0247	0.0329
	EMS	0.0173	0.0138	0.0193	0.019
	FIRE	0.0183	0.0107	0.0202	0.0246
	LE	0.0111	0.0172	0.0096	0.0113
	ALL	0.8375	0.8182	0.8385	0.8589
	ECC	0.8281	0.816	0.8254	0.8444
	EM	0.796	0.7798	0.7995	0.8125
	EMS	0.8301	0.8115	0.8287	0.8537
	FIRE	0.834	0.8235	0.8295	0.8522
	LE	0.8493	0.8113	0.8669	0.8646

Point Estimates 70 Rev. 2024.07.16

Point Estimates 99 Rev. 2024.07.16



Devin Christensen
September 19, 2024



For more information on the SNS:

cisa.gov/sns
sns@cisa.dhs.gov

devin.christensen@mail.cisa.dhs.gov

Devin Christensen
September 19, 2024

8





State of Minnesota Contract

SWIFT Contract Number: 251669

This Contract is between the State of Minnesota, acting through its Commissioner of Administration ("State") and RapidDeploy, Inc. whose designated business address is 310 Comal St, Building A, Suite 200, #205, Austin, TX 78702 ("Contractor"). State and Contractor may be referred to jointly as "Parties."

Recitals

1. State issued a solicitation identified as G0210-2000015106 on November 18th 2023 for 911 Automatic Location Identification (ALI) Solution ("Solicitation");
2. Contractor provided a response to the Solicitation indicating its interest in and ability to provide the goods or services requested in the Solicitation; and
3. Subsequent to an evaluation in accordance with the terms of the Solicitation, the Parties desire to enter into a contract.

Accordingly, the Parties agree as follows:

Contract

1. Term of Contract

- 1.1 Effective date. July 01, 2024, or the date the State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later. The Contractor must not begin work under this Contract until this Contract is fully executed and the Contractor has been notified by the State's Authorized Representative to begin the work.
- 1.2 Expiration date. July 31, 2026, or until all obligations have been satisfactorily fulfilled, whichever occurs first. The contract may be extended for up to an additional 60 months in increments as determined by the State, through a duly executed amendment.
- 1.3 Contract Use. This Contract is not exclusive and shall not be construed as guaranteeing a minimum or maximum amount of usage.

2. Contractor's Duties

The Contractor shall perform all duties described in this Contract to the satisfaction of the State.

3. Representations and Warranties

- 3.1 Under Minn. Stat. §§ 15.061 and 16C.03, subd. 3, and other applicable law the State is empowered to engage such assistance as deemed necessary.

3.2 Contractor warrants that it is duly qualified and shall perform its obligations under this Contract in accordance with the commercially reasonable standards of care, skill, and diligence in Contractor's industry, trade, or profession, and in accordance with the specifications set forth in this Contract, to the satisfaction of the State.

3.3 Contractor warrants that it possesses the legal authority to enter this Contract and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Contract, or any part thereof, and to bind Contractor to its terms.

4. Time

The Contractor must comply with all the time requirements described in this Contract. In the performance of this Contract, Contractor shall use commercially reasonable efforts to comply with all agreed upon timelines.

5. Compensation and Conditions of Payment

5.1 Compensation. The State will pay for performance by the Contractor under this Contract in accordance with the breakdown of costs as set forth in Exhibit D which is attached and incorporated into this Contract.

5.2 Conditions of Payment. All duties performed by the Contractor under this Contract must be performed to the State's satisfaction and in accordance with all applicable federal, state, and local laws, ordinances, rules, and regulations including business registration requirements of the Office of the Secretary of State. The Contractor will not receive payment for work found by the State to be unsatisfactory, provided that Contractor will be provided with the opportunity to correct any unsatisfactory work, or performed in violation of federal, state, or local law.

6. Authorized Representative

6.1 The State's Authorized Representative is Matt Hassenstab, Acquisition Management Specialist, Matt.Hassenstab@state.mn.us or his/her successor or delegate, and has the responsibility to monitor the Contractor's performance.

6.2 Contractor's Authorized Representative. The Contractor's Authorized Representative is Dami Bullock, Chief Revenue Officer, at the following business address and telephone number: 310 Comal Street, Building A, Suite 200 #205, Austin, TX 78702. Phone: (737) 201-9175, or his/her successor. If the Contractor's Authorized Representative changes at any time during this Contract, the Contractor must immediately notify the State.

7. Exhibits

The following Exhibits are attached and incorporated into this Contract. In the event of a conflict between the terms of this Contract and its Exhibits, or between Exhibits, the order of precedence is first the Contract, and then in the following order:

Exhibit A: Contract Terms

Exhibit B: Insurance Requirements

Exhibit C: Specifications, Duties, and Scope of Work

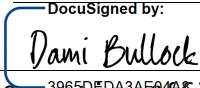
Exhibit D: Price and Payment Schedule

Exhibit E: Contractor Attachments

1. Contractor
The Contractor certifies that the appropriate person(s) have executed the Contract on behalf of the Contractor as required by applicable articles, bylaws, resolutions, or ordinances.5

Dami Bullock

Print name: _____

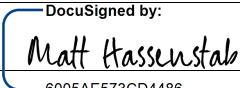
Signature:  _____
DocuSigned by: 3965DEDA3AE64A...

Title: Chief operating officer Date: 7/26/2024

2. State Agency
With delegated authority

Matt Hassenstab

Print name: _____

Signature:  _____
DocuSigned by: 6005AE573CD4486...

Title: Acquisition Management Specialist Date: 7/30/2024

3. Commissioner of Administration
As delegated to The Office of State Procurement
Andy Doran

Print name: _____

Signature:  _____
DocuSigned by: 68D02A26D7604BA...

Title: IT Acquisitions Supervisor Date: 7/30/2024

Exhibit A: Contract Terms

1. Prompt Payment and Invoicing.

- 1.1 Prompt Payment. The State will pay the Contractor pursuant to Minn. Stat. § 16A.124, which requires payment within 30 days following receipt of an undisputed invoice, or merchandise or service, whichever is later. Terms requesting payment in less than 30 days will be changed to read “Net 30 days.”
Notwithstanding the foregoing, the State may pay the Contractor in advance for purchases as allowed pursuant to Minn. Stat. §16A.065.

The payment for each order will only be made for goods received or services actually performed that have been accepted by the ordering entity, and meet all terms, conditions, and specifications of the Contract and the ordering document.

- 1.2 Invoicing. The invoice must be in the same format as the sample invoice form approved as Exhibit D, Supplement 1 with the Contract, unless an alternative format is approved in writing by the State Authorized Representative, or delegate. See Exhibit D, Supplement 1 for a list of minimum invoice requirements.

2. Assignment, Amendments, Waiver, and Contract Complete.

- 2.1 Assignment. The Contractor may neither assign nor transfer any rights or obligations under this Contract without the prior consent of the State provided that: (a) Contractor may assign its rights and obligations under this Agreement without the consent of the State, in connection with the sale of all or part of Contractor’s business, whether by merger or the sale or transfer of Contractor’s stock or assets; and (b) the State receives a fully executed assignment agreement, executed and approved by the authorized parties or their successors.
- 2.2 Amendments. Any amendment to this Contract must be in writing and will not be effective until it has been executed and approved by the authorized parties or their successors.
- 2.3 Waiver. If the State fails to enforce any provision of this Contract, that failure does not waive the provision or its right to enforce it.
- 2.4 Contract Complete. This Contract contains all negotiations and agreements between the State and the Contractor. No other understanding regarding this Contract, whether written or oral, may be used to bind either party.

3. Termination.

- 3.1 Termination for Convenience. The State or Commissioner of Administration may cancel this Contract at any time, with or without cause, upon 60 days’ written notice to the Contractor. Upon termination for convenience, the Contractor will be entitled to payment, determined on a pro rata basis, for services or goods satisfactorily performed or delivered. During the period between when notice is sent and the effective date of termination, the State shall continue to pay Contractor the fees then-currently in effect.
- 3.2 Termination for Breach. If the Contractor fails to perform according to the contract terms and conditions, the State is authorized to cancel the Contract or purchase order, or any portion of it, by providing thirty (30) days’ written notice to Contractor specifying in detail the nature of the breach, if Contractor does not cure such breach within that time period, and may obtain replacement goods or services and charge the difference of costs to the defaulting Contractor. In the event of default, the State reserves the right to pursue any other remedy available by law. A Contractor may be removed from the vendors list, suspended

or debarred from receiving a Contract for failure to comply with terms and conditions of the Contract, or for failure to pay the State for the cost incurred on the defaulted Contract.

3.3 Termination for Insufficient Funding. The State may immediately terminate this Contract if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued at a level sufficient to allow for the payment of the services addressed within this Contract. Termination must be by written notice to the Contractor. The State is not obligated to pay for any services that are provided after the effective date of termination (meaning 60 days after Contractor's receipt of written notice of termination). However, the Contractor will be entitled to payment, determined on a pro rata basis, for services satisfactorily performed to the extent that dedicated funds are available. The State will not be assessed any penalty if the Contract is terminated because of the decision of the Minnesota Legislature, or other funding source, not to appropriate funds. The State must provide the Contractor notice of the lack of funding. This notice will be provided within a reasonable time of the State's receiving notice.

4. Force Majeure.

Neither party shall be responsible to the other or considered in default of its obligations within this Contract to the extent that performance of any such obligations is prevented or delayed by acts of God, war, riot, disruption of government, or other catastrophes beyond the reasonable control of the party unless the act or occurrence could have been reasonably foreseen and reasonable action could have been taken to prevent the delay or failure to perform. A party relying on this provision to excuse performance must provide the other party prompt written notice of the inability to perform and take all necessary steps to bring about performance as soon as practicable.

5. Indemnification.

5.1 In the performance of this Contract, the Indemnifying Party must indemnify, save, and hold harmless the State, its agents, and employees, from any third-party claims or causes of action, including reasonable attorney's fees incurred by the State, to the extent caused by Indemnifying Party's:

- Intentional, willful, or negligent acts or omissions; or
- Actions that give rise to strict liability; or
- Breach of contract or warranty.

The Indemnifying Party is defined to include the Contractor, Contractor's reseller, any third party that has a business relationship with the Contractor, or Contractor's agents or employees, and to the fullest extent permitted by law. The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Indemnifying Party may have for the State's failure to fulfill its obligation under this Contract.

5.2 Nothing within this Contract, whether express or implied, shall be deemed to create an obligation on the part of the State to indemnify, defend, hold harmless or release the Indemnifying Party. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

6. Governing Law, Jurisdiction, and Venue.

Minnesota law, without regard to its choice-of-law provisions, governs this Contract. Venue for all legal proceedings out of this Contract, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

7. Contract Use by State Agencies.

To the extent applicable, the Contract does not prohibit state agencies from using their delegated purchasing authority to procure similar goods and services from other sources.

8. Warranty.

The Contractor warrants to the ordering entity that materials and equipment furnished under the Contract will be free from defects not inherent in the quality required or permitted, and that the work will conform to the requirements of the contract. Work not conforming to these requirements, including substitutions not properly approved and authorized in writing may be considered defective. The Contractor's warranty excludes remedy for damage or defect caused by abuse, modifications not executed by the Contractor, improper or insufficient maintenance, improper operation, or normal wear and tear and normal usage. If requested, the Contractor shall furnish satisfactory evidence as to the kind and quality of materials and equipment used.

All installation materials and labor shall be guaranteed for a period of one (1) year following the date of final acceptance. During the first year following acceptance, the Contractor shall, upon notification by the ordering entity of any malfunctions, make necessary repairs, including labor, travel, and materials, at the Contractor's expense.

OTHER THAN THE WARRANTIES SET FORTH IN THIS CONTRACT, TO THE MAXIMUM EXTENT PERMITTED BY LAW, CONTRACTOR, FOR ITSELF AND ON BEHALF OF ITS LICENSORS AND SUPPLIERS, DISCLAIMS ALL WARRANTIES RELATING TO THE SERVICES OR TO ANY MATERIALS OR SERVICES PROVIDED TO THE STATE UNDER THIS AGREEMENT (INCLUDING ANY THIRD PARTY CONTENT), WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CONTRACTOR, ITS LICENSORS AND SUPPLIERS DO NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR FREE FROM DEFECTS OR ERRORS, OR THAT THE SERVICES WILL MEET (OR ARE DESIGNED TO MEET) THE STATE'S REQUIREMENTS.

9. Original Equipment Manufacturer (OEM Warranty).

The equipment offered must include the OEM standard warranty. The Contractor is responsible for the cost of any inspections, adjustments, warranted parts, and labor charges to repair or replace warranted parts that are a result of equipment failure(s) during the warranty period. This shall be performed promptly unless otherwise mutually agreed in writing by the Customer and the Contractor. This warranty shall commence when the unit is put into service.

9.1 OEM Extended Warranty Options. If the Contractor provides an OEM Extended Warranty Option, the Contractor must provide a copy of the applicable terms and conditions, including a detail of coverage, to the State upon request. The cost of an OEM Extended Warranty must include all associated costs.

9.2 Contractor (Add-On) Warranty Options. The Contractor may provide additional warranty options, which include, but are not limited to travel pickup, or delivery charges that are a result of equipment failure(s) prior to or during the warranty period or extended warranty period. This warranty option shall commence when the unit is put into service and is in addition to OEM warranty options stated above.

10. Delivery.

Contractor is obligated to deliver within the quoted lead times. If delivery is not made within that time frame, the State reserves the right to deem the Contractor in default.

Contractor must confirm delivery locations and requirements with the ordering entity. Prior to delivery, the Contractor is responsible for confirming in writing with the ordering entity that the delivery location will accommodate unloading the equipment. Contractor must notify the receiving entity at least 72 hours before delivery to allow for inspection and compliance. No delivery can be made on a State Holiday (as defined in Minn. Stat. § 645.44, subd. 5), on Saturday or Sunday, or after 4:00 p.m. Central Time on weekdays, without prior written approval by the receiving entity.

11. Risk of Loss.

The State is relieved of all risks of loss or damage to the goods and equipment during periods of transportation, installation by the Contractor, or while in the possession of the Contractor or its agent.

12. Purchase Orders.

The parties agree that there is no minimum order requirements or charges to process an individual purchase order unless otherwise stated in the Contract. The Purchase Order number must appear on all documents (e.g., invoices, packing slips, etc.).

13. Equipment Specifications.

All equipment must meet the contract specifications and all federal and State safety codes and regulations in effect at the date of manufacture. All equipment must be Original Equipment Manufacturer (OEM) equipment unless otherwise stated in the contract.

14. Items Offered as New.

All products, materials, supplies, replacement parts, and equipment offered and furnished must be new, of current manufacturer production, and must have been formally announced by the manufacturer as being commercially available, unless otherwise stated in this Contract.

15. Subcontracting and Subcontractor Payment.

- 15.1 Subcontracting Allowed. A subcontractor is a person or company that has been awarded a portion of the Contract by Contractor. Only subcontractors that have been approved by the State's Authorized Representative can be used for this Contract.

After the effective date of the Contract, the Contractor shall not, without prior written approval of the State's Authorized Representative, subcontract for the performance of any of the Contractor's obligations that were not already approved for subcontracting when the Contract was awarded. During this Contract, if an approved subcontractor is determined to be performing unsatisfactorily by the State's Authorized Representative, the Contractor will receive written notification that the subcontractor can no longer be used for this Contract.

The provisions of the Contract shall apply with equal force and effect to all approved subcontractors engaged by the Contractor. Notwithstanding approval by the State, no subcontract shall serve to terminate or in any way affect the primary legal responsibility of the Contractor for timely and satisfactory performances of the obligations contemplated by the Contract.

- 15.2 Subcontractor Payment. Contractor must pay any subcontractor in accordance with Minn. Stat. § 16A.1245.

Data Disclosure.

Under Minn. Stat. § 270C.65, subd. 3 and other applicable law, the Contractor consents to disclosure of its social security number, federal employer tax identification number, and Minnesota tax identification number, already provided to the State, to federal and state agencies, and state personnel involved in the payment of state obligations. These identification numbers may be used in the enforcement of federal and state laws which could result in action requiring the Contractor to file state tax returns, pay delinquent state tax liabilities, if any, or pay other state liabilities.

16. Government Data Practices.

The Contractor and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (or, if the State contracting party is part of the Judicial Branch, with the Rules of Public Access to Records of the Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by the State under this Contract, and as it applies to all data created, collected, received, stored, used,

maintained, or disseminated by the Contractor under this Contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. Ch. 13, by either the Contractor or the State.

If the Contractor receives a request to release the data referred to in this clause, the Contractor must immediately notify and consult with the State's Authorized Representative as to how the Contractor should respond to the request. The Contractor's response to the request shall comply with applicable law.

17. Intellectual Property Rights.

17.1 Definitions. For the purpose of this Section, the following words and phrases have the assigned definitions:

17.1.1 "Documents" are the originals of any databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, disks, or other materials, whether in tangible or electronic forms, prepared by the Contractor, its employees, agents, or subcontractors, in the performance of this Contract.

17.1.2 "Pre-Existing Intellectual Property" means intellectual property developed prior to or outside the scope of this Contract, and any modifications, upgrades, improvements and/or derivatives of that intellectual property.

17.1.3 "Works" means all inventions, improvements, discoveries (whether or not patentable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by the Contractor, its employees, agents, and subcontractors, either individually or jointly with others in the performance of this Contract. "Works" includes Documents.

17.2 Ownership. Except with respect to Contractor's Pre-existing Intellectual Property, the State owns all rights, title, and interest in all of the intellectual property rights, including copyrights, patents, trade secrets, trademarks, and service marks in the Works and Documents created and paid for under this Contract. The Documents shall be the exclusive property of the State and all such Documents must be immediately returned to the State by the Contractor upon completion or cancellation of this Contract. To the extent possible, those Works eligible for copyright protection under the United States Copyright Act will be deemed to be "works made for hire." The Contractor assigns all right, title, and interest it may have in the Works and the Documents to the State. The Contractor must, at the request of the State, execute all papers and perform all other acts necessary to transfer or record the State's ownership interest in the Works and Documents. For the avoidance of doubt, any intellectual property rights related to integrations with third-party data sources and/or partner solutions shall be part of Contractor's Pre-existing Intellectual Property.

17.3 Pre-existing Intellectual Property. Each Party shall retain ownership of its respective Pre-Existing Intellectual Property. The Contractor grants the State a perpetual, irrevocable, non-exclusive, royalty free license for Contractor's Pre-Existing Intellectual Property that are incorporated in the products, materials, equipment, deliverables, or services that are purchased through the Contract.

17.4 Obligations.

- 17.4.1 Notification. Whenever any invention, improvement, or discovery (whether or not patentable) is made or conceived for the first time or actually or constructively reduced to practice by the Contractor, including its employees and subcontractors, in the performance of this Contract, the Contractor will immediately give the State's Authorized Representative written notice thereof, and must promptly furnish the State's Authorized Representative with complete information and/or disclosure thereon.
- 17.4.2 Representation. The Contractor must perform all acts, and take all steps necessary to ensure that all intellectual property rights in the Works and Documents are the sole property of the State, and that neither Contractor nor its employees, agents, or subcontractors retain any interest in and to the Works and Documents. The Contractor represents and warrants that the Works and Documents do not and will not infringe upon any intellectual property rights of other persons or entities.
- 17.4.3 Indemnification. Notwithstanding any other indemnification obligations addressed within this Contract, the Contractor will indemnify; defend, to the extent permitted by the Attorney General; and hold harmless the State, at the Contractor's expense, from any action or claim brought against the State to the extent that it is based on a claim that all or part of the Works or Documents infringe upon the intellectual property rights of others. The Contractor will be responsible for payment of any and all such claims, demands, obligations, liabilities, costs, and damages, including but not limited to, attorney fees. If such a claim or action arises, or in the Contractor's or the State's opinion is likely to arise, the Contractor must, at the State's discretion, either procure for the State the right or license to use the intellectual property rights at issue or replace or modify the allegedly infringing works or documents as necessary and appropriate to obviate the infringement claim. If the foregoing are commercially impracticable, Contractor shall refund to the State any amounts pre-paid for the allegedly infringing works. This remedy of the State will be in addition to and not exclusive of other remedies provided by law.

18. Copyright.

The Contractor shall save and hold harmless the State of Minnesota, its officers, agents, servants and employees, from liability of any kind or nature, arising from the use of any copyrighted or noncopyrighted compositions, secret process, patented or nonpatented invention, article or appliance furnished or used in the performance of the Contract.

19. Assignment of Antitrust Rights.

Upon the request of the State of Minnesota, Contractor will irrevocably assign to State any state or federal antitrust claim or cause of action that the Contractor now has or which may accrue to the Contractor in the future, in connection with any goods, services, or combination provided by Contractor under the terms of this Contract.

20. Survivability of Orders.

In the event the term of any order or Professional/Technical Services work order ("Order") placed under this Contract extends past the termination or expiration of this Contract, the terms and conditions of this Contract shall remain in full force and effect as it applies to such order and will continue in effect for such order until the term of that order expires or the order is cancelled or terminated in accordance with the terms of this Contract.

21. Contractor's Documents.

Any licensing and maintenance agreement, or any order-specific agreement or document, including any pre-installation, linked or "click through" agreement that is allowed by, referenced within or incorporated within the Contract whenever the Contract is used for a State procurement, whether directly by the Contractor or through a Contractor's agent, subcontractor or reseller, is agreed to only to the extent the terms within any such agreement or document do not

conflict with the Contract or applicable Minnesota or Federal law, and only to the extent that the terms do not modify, diminish or derogate the terms of the Contract or create an additional financial obligation to the State. Any such agreement or document must not be construed to deprive the State of its sovereign immunity, or of any legal requirements, prohibitions, protections, exclusions or limitations of liability applicable to this Contract or afforded to the State by Minnesota law. A State employee's decision to choose "accept" or an equivalent option associated with a "click-through" agreement does not constitute the State's concurrence or acceptance of terms, if such terms are in conflict with this section.

22. State Audits.

Under Minn. Stat. § 16C.05, subd. 5, the Contractor's books, records, documents, and accounting procedures and practices relevant to this Contract are subject to examination by the State, the State Auditor, or Legislative Auditor, as appropriate, for a minimum of six years from the expiration or termination of this Contract.

23. Usage Reports.

Contractor must track and report to the State usage data on this Contract (Usage Reports). Usage Reports should be sent via email to osp.usagereports@state.mn.us. A Usage Report must identify the State Contract Number and provide the following information:

- The total amount of spend under the Contract by the State and other entities,
- The total amount of spend by State agencies, and
- The total amount of spend by other entities (CPV members).

Contractor must send a quarterly Usage Report, or as otherwise requested. Quarters are as follows:

- First Quarter, from July 1 to September 30,
- Second Quarter, from October 1 to December 31,
- Third Quarter, from January 1 to March 31, and
- Fourth Quarter, from April 1 to June 30.

A quarterly Usage Report is due within thirty days of the end of a quarter. A requested Usage Report is due within thirty days from when the request was made. Contractor must provide the State with a final Usage Report within 30 calendar days of the expiration or termination of the Contract. Failure to provide a Usage Report may result in the State cancelling the Contract. This term survives the expiration or termination of the Contract.

24. Diverse Spend Reporting.

If the total value of the Contract may exceed \$500,000, including all extension options, Contractor must track and report, on a quarterly basis, the amount paid to diverse businesses both: 1) directly to subcontractors performing under the Contract, and 2) indirectly to diverse businesses that provide supplies/services to your company (in proportion to the revenue from this Contract compared to Contractor's overall revenue). When this applies, Contractor will register in a free portal to help report the Tier 2 diverse spend, and the requirement continues as long as the Contract is in effect.

25. Publicity and Endorsement.

25.1 Publicity. Any publicity regarding the subject matter of this Contract must identify the State as the sponsoring agency and must not be released without prior written approval from the State's Authorized Representative. For purposes of this provision, publicity includes notices, informational pamphlets, press releases, information posted on corporate or other websites, research, reports, signs, and similar public notices prepared by or for the Contractor individually or jointly with others, or any subcontractors, with respect to the program, publications, or services provided resulting from this Contract.

25.2 Endorsement. The Contractor must not claim that the State endorses its products or services.

26. Debarment by State, its Departments, Commissions, Agencies, or Political Subdivisions.

Contractor certifies that neither it nor its principals is presently debarred or suspended by the Federal government, the State, or any of the State's departments, commissions, agencies, or political subdivisions. Contractor's certification is a material representation upon which the Contract award was based. Contractor shall provide immediate written notice to the State's Authorized Representative if at any time it learns that this certification was erroneous when submitted or becomes erroneous by reason of changed circumstances.

27. Contingency Fees Prohibited.

Pursuant to Minn. Stat. § 10A.06, no person may act as or employ a lobbyist for compensation that is dependent upon the result or outcome of any legislation or administrative action.

28. Certification of Nondiscrimination (in accordance with Minn. Stat. § 16C.053).

If the value of this Contract, including all extensions, is \$50,000 or more, Contractor certifies it does not engage in and has no present plans to engage in discrimination against Israel, or against persons or entities doing business in Israel, when making decisions related to the operation of the vendor's business. For purposes of this section, "discrimination" includes but is not limited to engaging in refusals to deal, terminating business activities, or other actions that are intended to limit commercial relations with Israel, or persons or entities doing business in Israel, when such actions are taken in a manner that in any way discriminates on the basis of nationality or national origin and is not based on a valid business reason.

29. Non-discrimination (in accordance with Minn. Stat. § 181.59).

The Contractor will comply with the provisions of Minn. Stat. § 181.59.

30. E-Verify Certification (in accordance with Minn. Stat. § 16C.075).

For services valued in excess of \$50,000, Contractor certifies that as of the date of services performed on behalf of the State, Contractor and all its subcontractors will have implemented or be in the process of implementing the federal E-Verify Program for all newly hired employees in the United States who will perform work on behalf of the State. Contractor is responsible for collecting all subcontractor certifications and may do so utilizing the [E-Verify Subcontractor Certification Form](#). All subcontractor certifications must be kept on file with Contractor and made available to the State upon request.

31. Affirmative Action Requirements

The State intends to carry out its responsibility for requiring affirmative action by its contractors.

- 31.1 Covered Contracts and Contractors. If the Contract exceeds \$100,000 and the Contractor employed 40 or more full-time employees on a single working day during the previous 12 months in Minnesota or in the state where it has its principal place of business, then the Contractor must comply with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600.
- 31.2 General. Minn. R. 5000.3400-5000.3600 implements Minn. Stat. § 363A.36. These rules include, but are not limited to, criteria for contents, approval, and implementation of affirmative action plans; procedures for issuing certificates of compliance and criteria for determining a contractor's compliance status; procedures for addressing deficiencies, sanctions, and notice and hearing; annual compliance reports; procedures for compliance review; and contract consequences for non-compliance. The specific criteria for approval or rejection of an affirmative action plan are contained in various provisions of Minn. R. 5000.3400-5000.3600 including, but not limited to, Minn. R. 5000.3420-5000.3500 and 5000.3552-5000.3559.
- 31.3 Disabled Workers. The Contractor must comply with the following affirmative action requirements for disabled workers.

AFFIRMATIVE ACTION FOR DISABLED WORKERS

- 31.3.1 The Contractor must not discriminate against any employee or applicant for employment because of physical or mental disability in regard to any position for which the employee or applicant for employment is qualified. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified disabled persons without discrimination based upon their physical or mental disability in all employment practices such as the following: employment, upgrading, demotion or transfer, recruitment, advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.
- 31.3.2 The Contractor agrees to comply with the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.
- 31.3.3 In the event of the Contractor's noncompliance with the requirements of this clause, actions for noncompliance may be taken in accordance with Minn. Stat. § 363A.36, and the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.
- 31.3.4 The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices in a form to be prescribed by the Commissioner. Such notices must state the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified disabled employees and applicants for employment, and the rights of applicants and employees.
- 31.3.5 The Contractor must notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of Minn. Stat. § 363A.36, of the Minnesota Human Rights Act and is committed to take affirmative action to employ and advance in employment physically and mentally disabled persons.

31.4 Consequences. The consequences for the Contractor's failure to implement its affirmative action plan or make a good faith effort to do so include, but are not limited to, suspension or revocation of a certificate of compliance by the Commissioner, refusal by the Commissioner to approve subsequent plans, and termination of all or part of this Contract by the Commissioner or the State.

31.5 Certification. The Contractor hereby certifies that it is in compliance with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600 and is aware of the consequences for noncompliance.

32. Equal Pay Certification.

If required by Minn. Stat. §363A.44, the Contractor must have a current Equal Pay Certificate prior to Contract execution. If Contractor's Equal Pay Certificate expires during the term of this Contract, Contractor must promptly re-apply for an Equal Pay Certificate with the Minnesota Department of Human Rights and notify the State's Authorized Representative once the Contractor has received the renewed Equal Pay Certificate. If Contractor claims to be exempt, the State may require Contractor to verify its exempt status.

33. Professional/Technical (P/T) Services Ancillary to Goods or General Services.

For state agencies, Professional/Technical (P/T) Services must be related to the goods or services purchased from this Contract and is limited to \$50,000 per project. Based on the size, scope and complexity of a project, the State's Authorized Representative may approve dollar limits exceeding \$50,000 per project. This may require a separate work order contract defining the PT scope of work.

Ten percent (10%) of the cost of each P/T deliverable will be withheld by the State. The retainage will be held by the State until the P/T deliverable has been reviewed by the head of the agency entering into the Contract and the head of the agency has certified that the Contractor has satisfactorily fulfilled the terms of the Contract.

34. Hazardous Substances.

To the extent that the goods to be supplied to the State by the Contractor contain or may create hazardous substances, harmful physical agents, or infectious agents, as set forth in applicable State and federal laws and regulations, the Contractor must provide the State with Material Safety Data Sheets regarding those substances. A copy must be provided upon request. Goods and containers supplied to the State must be labeled in compliance with state and federal laws, rules, and regulations.

These terms apply to goods supplied under this contract:

- 34.1 Products Containing Triclosan Banned. The Contractor must comply with Minn. Stat. § 145.945.
- 34.2 Products Containing Certain Types of Polybrominated Diphenyl Ether Banned. The Contractor must comply with Minn. Stat. § 325E.385-325E.388).
- 34.3 Coal Tar Sealant Use and Sale Prohibited. The Contractor must comply with Minn. Stat. § 116.202.
- 34.4 Products Containing Mercury. The Contractor must comply with Minn. Stat. 116.92.

35. IT Accessibility Standard.

Contractor acknowledges and is fully aware that the State of Minnesota (Executive branch state agencies) has developed its IT Accessibility Standard effective September 1, 2010. The Standard entails, in part, the Web Content Accessibility Guidelines (WCAG) and Section 508 which can be viewed at: <https://mn.gov/mnit/government/policies/accessibility/>.

The Standard applies to web sites, software applications, electronic reports and output documentation, training delivered in electronic formats (including, but not limited to, documents, videos, and webinars), among others. As upgrades are made to the software, products, or subscriptions available through this Contract, the Contractor agrees to develop functionality which supports accessibility. If any issues arise due to nonconformance with the above-mentioned accessibility Standard, the Contractor agrees to provide alternative solutions upon request at no additional charge to the State.

When updates or upgrades are made to the products or services available through this Contract, the Contractor agrees to document how the changes will impact or improve the product or service's accessibility and usability. This documentation, upon request, must be provided to the State in advance of the change, occurring within an agreed upon timeframe sufficient for the state to review the changes and either approve them or request a remediation plan from the Contractor. Contractor warrants that it will use commercially reasonable efforts to have the Products comply with the above-mentioned accessibility Standards taking into account the nature of the products that are being provided to the State and agrees to indemnify, defend, and hold harmless the State against any claims related to non-compliance of Contractor's Product with the above-mentioned accessibility Standard. If agreed-upon updates fail to improve the product or service's accessibility or usability as planned, the failure to comply with this requirement may be cause for contract cancellation or for the State to consider the Contractor in default.

36. Security and Data Protection.

Contractor is responsible for the security and protection of State data subject to and related to Cloud Services in this Contract. The terms, conditions, and provisions of this Security and Data Protection section take precedence and will prevail over any other terms, conditions, and provisions of the Contract, if in conflict. This Security and Data Protection section, including its sub-sections, survives the completion, termination, expiration, or cancellation of the Contract.

36.1 For the purposes of this Security and Data Protection section, the following terms have the following meanings:

36.1.1 "Cloud Services" includes "cloud computing" as defined by the U.S. Department of Commerce, NIST Special Publication 800-145 (currently available online at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>) and any other software, hardware, hosting service, subscription, or other service or product by which Contractor stores, transmits, processes or otherwise has access to State data.

36.1.2 "State" means the State, or a cooperative purchasing venture ("CPV") member when the CPV member is the ordering entity (if CPV purchases are permitted under this Contract).

36.1.3 "Data" has the meaning of "government data" in Minn. Stat. § 13.02, subd. 7.

36.1.4 "Not public data" has the meaning in Minn. Stat. § 13.02, subd. 8a.

36.1.5 "Security incident" means any actual, successful or suspected: (1) improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, modification of, alteration to, loss of, damage to or destruction of State data; (2) interference with an information system; (3) disruption of or to Contractor's service(s); or (4) any similar or related incident.

36.1.6 "Privacy incident" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); violation of federal data disclosure or privacy requirements in federal laws, rules and regulations; or breach of a contractual obligation to protect State data. This includes, but is not limited to, improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, damage to, loss of, modification of, alteration to or destruction of State data protected by such State or federal laws or by contract.

36.2 Data Ownership. The State solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all State data. Contractor has no and acquires no right, title or interest, whether express or implied, in and to State data.

Contractor will only use State data for the purposes set forth in the Contract. Contractor will only access State data as necessary for performance of this Contract. Contractor will not access State user accounts except to respond to service or technical problems or at the State's specific request.

All State data, including copies, summaries and derivative works thereof, must be remitted, in a mutually agreeable format and media, to the State by the Contractor upon request or upon completion, termination or cancellation of the Contract. The foregoing sentence does not apply if the State Chief Information Security Officer or delegate authorizes in writing the Contractor to sanitize or destroy the data and the Contractor certifies in writing the sanitization or destruction of the data. Within ninety days following any remittance of State data to the State,

Contractor shall, unless otherwise instructed by the State in writing, sanitize or destroy any remaining data and certify in writing that the sanitization or destruction of the data has occurred. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

In the event Contractor receives a request to release any State data, Contractor must immediately notify the State's data practices compliance official. The State will give Contractor instructions concerning the release of the data to the requesting party before the data is released. Contractor must comply with the State's instructions. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data by Contractor.

36.3 Notification of Incidents. If Contractor becomes aware of or has reasonable suspicion of a privacy incident or security incident regarding any State data, Contractor must report such incident to the State and the State Chief Information Security Officer as soon as possible, but no later than twenty-four (24) hours after such incident. The decision to notify the affected data subjects and the form of such notice following report of a privacy incident or security incident are the responsibility of the State. Notwithstanding anything to the contrary in this Contract, Contractor will indemnify, hold harmless and defend the State and its officers, and employees for and against any claims, damages, costs and expenses related to any privacy incident or security incident involving any State data. For purposes of clarification, the foregoing sentence shall in no way limit or diminish Contractor's obligation(s) to indemnify, save, hold harmless, or defend the State under any other term of this Contract. Contractor will reasonably mitigate any harmful effects resulting from any privacy incident or security incident involving any State data.

36.4 Security Program. Contractor will make best efforts to protect and secure the State data related to this Contract. Contractor will establish and maintain an Information Security Program ("Program") that includes an information security policy applicable to any and all Cloud Services ("Policy"). Contractor's Program and Policy must align with appropriate industry security frameworks and standards such as National Institute of Standards and Technology ("NIST") 800-53 Special Publication Revision 5, Federal Information Processing Standards ("FIPS") 199, Federal Risk and Authorization Management Program ("FedRamp"), or Control Objectives for Information and Related Technology ("COBIT").

Upon the State's request, Contractor will make its Policy available to the State on a confidential, need-to-know basis, along with other related information reasonably requested by the State regarding Contractor's security practices and policies. Unless inconsistent with applicable laws, Contractor and the State must treat the Policy and related information on security practices and policies that are specific to the State as confidential information and as not public data pursuant to Minn. Stat. § 13.37.

36.5 Data Management. Contractor will not use State data, including production data, for testing or development purposes unless authorized in writing by the State Chief Information Security Officer or delegate. Contractor will implement and maintain procedures to physically and logically segregate State data, unless otherwise explicitly authorized by the State Chief Information Security Officer or delegate.

36.6 Data Encryption. Contractor must encrypt all State data at rest and in transit, in compliance with FIPS Publication 140-2 or applicable law, regulation or rule, whichever is a higher standard. All encryption keys must be unique to State data. Contractor will secure and protect all encryption keys to State data. Encryption keys to State data will only be accessed by Contractor as necessary for performance of this Contract.

36.7 Data Storage. Contractor warrants that any and all State data will be stored, processed, and maintained solely on designated servers and that no such data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is in use as part of the Contractor's designated backup and recovery processes.

36.8 Data Center and Monitoring/Support Locations. During the term of the Contract, Contractor will: (1) locate all production and disaster recovery data centers that store, process or transmit State data only in the continental United States, (2) store, process and transmit State data only in the continental United States, and (3) locate all monitoring and support of all Cloud Services only in the continental United States. The State has the right to on-site visits and reasonable inspection of the data centers upon notice to Contractor of seven calendar days prior to visit.

36.9 Security Audits & Remediation. Contractor will audit the security of the systems and processes used to provide any and all Cloud Services, including those of the data centers used by Contractor to provide any and all Cloud Services to the State. This security audit: (1) will be performed at least once every calendar year beginning with 2016; (2) will be performed according Statement on Standards for Attestation Engagements (“SSAE”) 16 Service Organization Control (“SOC”) 2, International Organization for Standardization (“ISO”) 27001, or FedRAMP; (3) will be performed by third party security professionals at Contractor’s election and expense; (4) will result in the generation of an audit report (“Contractor Audit Report”), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section.

Upon the State’s reasonable, advance written request, Contractor will provide to the State a copy of the Contractor Audit Report.

Contractor will make best efforts to remediate any control deficiencies identified in the Contractor Audit Report in a commercially reasonable timeframe.

If the State becomes aware of any other Contractor controls that do not substantially meet the State’s requirements, the State may request remediation from Contractor. Contractor will make best efforts to remediate any control deficiencies identified by the State or known by Contractor, in a commercially reasonable timeframe.

36.10 Insurance and Liability. Contractor warrants that it has and will maintain the insurance described below in force and effect throughout the term of the Contract. An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor’s policy limits to satisfy the full policy limits required by the Contract provided that Contractor warrants that the minimum coverage requirements below are met.

Professional/Technical, Errors and Omissions, including Network Security and Privacy Liability Insurance (or equivalent Network Security and Privacy Liability coverage endorsed on another form of liability coverage or written as a standalone policy):

This policy must provide coverage for all claims Contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to the Contract, including but not limited to claims which may arise from failure of Contractor’s or a subcontractor’s security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of confidential or private information, transmission of a computer virus or denial of service.

Contractor is required to carry the following minimum limits:

\$2,000,000 – per claim or event
\$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the Contractor and, unless Contractor maintains an audited net worth of at least \$100 million, the deductible may not exceed \$100,000 without the written approval of the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so

request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources. The retroactive or prior acts date of such coverage shall not be after the effective date of the Contract. Contractor shall maintain such insurance for a period of at least three (3) years following expiration or termination of the Contract. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract. If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor will notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State. Contractor is responsible for payment of Contract related insurance premiums and deductibles. If Contractor is self-insured, a Certificate of Self-Insurance must be provided to the State. Contractor shall obtain insurance policy(ies) from insurance company(ies) having an "AM BEST" rating of A- (minus); Financial Size Category ("FSC") VII or better, and authorized to do business in the State. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's authorized representative upon written request. The State reserves the right to immediately terminate the Contract if the Contractor is not in compliance with the insurance requirements of this sub-section and retains all rights to pursue any legal remedies against the Contractor.

Notwithstanding any limitation of liabilities in the Contract, the Contractor shall be liable for all damages to the extent such damages are within the insurance limit.

36.11 Subcontractors and Third Parties. Contractor warrants that no State data will be transmitted, exchanged or otherwise provided to other parties except as specifically agreed to in writing by the State Chief Information Security Officer or delegate. Contractor must ensure that any contractors, subcontractors, agents and others to whom it provides State data, agree in writing to be bound by the same restrictions and conditions under this Contract that apply to Contractor with respect to such data.

36.12 Compliance with Data Privacy and Security Laws and Standards. Contractor shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations.

36.13 Remedies. Contractor acknowledges that the State, because of the unique nature of its data, would suffer irreparable harm in the event that Contractor breaches its obligation under this Security and Data Protection section, and monetary damages may not adequately compensate the State for such a breach. In such circumstances, the State will be entitled, in addition to monetary relief, to injunctive relief or specific performance as may be necessary to restrain any continuing or further breach by Contractor, without showing or proving any actual damages sustained by the State.

36.14 Business Continuity. Contractor shall have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that Cloud Services provided under this Contract shall be maintained continuously in the event of a disruption to the Contractor's operations, regardless of the cause of the disruption. Such plans must, at a minimum, define the Contractor's actions to address the impacts of the following key areas likely to cause a disruption to Contractor's operations: loss of key personnel, loss of facility, and loss of information technology. Contractor must conduct testing and review of its business continuity and disaster recovery plan at least annually. Upon State request, Contractor must also participate, at mutually agreed upon times, in State business continuity and disaster recovery testing, training, and exercise activities.

Any term or condition that allows the Contractor to terminate the Contract for any or no reason (i.e., termination for convenience) is null and void. In the event of termination or cancellation of this Contract for any reason, the

Contractor shall continue to provide any then-existing Cloud Services for as long as the State needs to transfer its data, software and other assets to an alternate service or service provider. After any such termination or cancellation, the State may purchase the continuing Cloud Services at the pricing in effect prior to such termination or cancellation. The fee for any such purchase shall be prorated for the period of time needed, as determined by the State, and shall be reduced by the amount paid for Cloud Services that were not used prior to such termination or cancellation. The amount of any such fee reduction shall be determined on a pro-rata basis. The Contractor shall refund to the State any unused portion of payments for Cloud Services.

36.15 Background Checks. Contractor represents that it has conducted and will conduct background investigations into all of Contractor's agents, employees, and subcontractors that will provide Cloud Services to the State. Such background investigations must have been or will be conducted by investigating local, state and federal criminal records, local, state and federal civil case records, and employment references.

If any provision of this sub-section is found to violate any applicable laws, rules, or State policies, then the Contractor will be relieved of all obligations arising under such provision. Notwithstanding anything to the contrary in this sub-section, this sub-section is only applicable and effective to extent that it is consistent with applicable laws, rules, and State policies.

36.16 Secure Coding. Contractor will use reasonable commercial efforts to keep all Cloud Services free from any and all critical defects in materials, workmanship, and design. Contractor warrants that all Cloud Services are free from known viruses, malware, and other harmful or malicious code. Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made and again before being placed into production, and must promptly remediate any critical vulnerabilities. Contractor must follow best practices for application code review and the most current version of the OWASP top 10.

36.17 Compliance with Data Privacy and Security Laws and Standards. Contractor shall comply with the applicable State of Minnesota Information Security Policy & Standards incorporated herein by reference and available at <https://mn.gov/mnit/government/policies/security/>.

Contractor shall comply with the Health Insurance Portability Accountability Act ("HIPAA"), the HITECH Act, and other similar privacy laws. Contractor also shall comply with the HIPAA Privacy Rule, HIPAA Security Rule, and other similar rules, regulations, and laws, including future amendments thereto.

Contractor shall comply with all applicable requirements, restrictions, and conditions set forth in the Criminal Justice Information Services ("CJIS") – Security Policy, Version 5.3, dated 8/4/2014, including, but not limited to, conducting FBI fingerprint background checks on all of Contractor's agents, employees, and subcontractors that have or will have access to Criminal Justice Information ("CJI").

Contractor acknowledges that for the purposes of this Contract when storing, processing, transmitting or otherwise accessing State data subject to the Family Educational Rights and Privacy Act ("FERPA"), it is designated as a "school official" with "legitimate educational interests" in State data and associated metadata, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Contractor shall use State data only for the purpose of fulfilling its duties under the Contract and it will not monitor or share such data with or disclose it to any third party except as provided for in this Contract, as required by law, or as authorized in writing by the State. By way of illustration and not of limitation, Contractor will not use such data for Contractor's own benefit and, in particular, will not engage in "data mining" of such data or communications, whether through automated or human means, except as necessary to fulfill its duties under this Contract, or as specifically and expressly provided for in this Contract, as required by law, or authorized in writing by the State. Contractor agrees, upon request, to provide the State with a written summary of the procedures Contractor uses to safeguard State data.

All of Contractor's systems and components that process, store, or transmit Cardholder Data shall comply with the most recent version of the Payment Card Industry Data Security Standard ("PCI DSS") promulgated by the PCI Security Standards Council, currently available online at: https://www.pcisecuritystandards.org/document_library. The Contractor shall, upon request, provide the State with Contractor's current Attestation of Compliance signed by a PCI QSA ("Qualified Security Assessor"). For purposes of this sub-section, "Cardholder Data" has the meaning defined by the PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), Glossary of Terms, Abbreviations, and Acronyms, currently available online at: https://www.pcisecuritystandards.org/document_library.

Contractor shall comply with IRS Publication 1075, Exhibit 7, which is incorporated herein.

For the term of this Contract, Contractor will maintain a StateRAMP Progressing SnapShot, working towards StateRAMP Authorized (Moderate) or Federal Agency for any and all Cloud Services provided under this Contract. The Contractor host the application(s) on Microsoft Azure Government which is compliant with the Federal Risk and Authorization Management Program (FedRAMP). Azure Government has been designed specifically for U.S. government agencies and their partners, meet the requirements for FedRAMP High.

For the term of this Contract, Contractor will maintain an ISO 27001 Certification for any and all Cloud Services provided under this Contract.

36.18 The State authorizes Contractor to provide "other emergency communications services" and acknowledges and agrees that Contractor is and shall be an "other emergency communications service provider" in accordance with U.S. Code Title 47., Chapter 5., Subchapter VI., 615b and shall be subject to the immunities and other protections from liability set forth in U.S. Code Title 47., Chapter 5., Subchapter VI., 615b.

36.19 CONTRACTOR'S LIABILITY IS LIMITED AS FOLLOWS: (I) IN THE EVENT ANY SUCH LIABILITY OR CLAIM IS OR SHOULD HAVE BEEN COVERED BY AN INSURANCE POLICY SECURED BY CONTRACTOR AS REQUIRED BY THIS CONTRACT, THEN SUCH LIABILITY OR CLAIM WILL BE LIMITED TO THE AMOUNT OF ACTUAL OR REQUIRED COVERAGE, WHICHEVER IS GREATER; AND, (II) PROVIDED THAT THE CONTRACTOR COMPLIED WITH ITS INSURANCE OBLIGATIONS AS REQUIRED BY THIS CONTRACT, IN THE EVENT ANY SUCH LIABILITY OR CLAIM IS NOT COVERED BY AN INSURANCE POLICY SECURED BY CONTRACTOR, THEN THE LIABILITY AND CLAIMS WILL BE LIMITED TO AN AMOUNT EQUAL TO THE AMOUNT OF FEES ACTUALLY PAID BY STATE TO CONTRACTOR IN THE LAST TWENTY-FOUR (24) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM; PROVIDED, HOWEVER, THAT THE FOREGOING CLAUSE (II) IS NOT INTENDED, AND WILL NOT BE DEEMED, TO LIMIT OR RESTRICT IN ANY WAY ANY COVERAGE OR BENEFITS PROVIDED UNDER ANY APPLICABLE INSURANCE POLICY SECURED BY CONTRACTOR. STATE MAY BE ADDED AS AN ADDITIONAL INSURED ON CONTRACTOR'S CERTIFICATE OF INSURANCE UPON REQUEST. THE FOREGOING EXCLUSIONS AND LIMITATIONS OF LIABILITY WILL NOT APPLY TO: (I) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; (II) INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT; (III) EITHER PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS HEREUNDER; (IV) STATE'S INFRINGEMENT, MISAPPROPRIATION OR OTHER VIOLATION OF CONTRACTOR'S INTELLECTUAL PROPERTY RIGHTS, OR (V) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY LAW.

36.20 TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND UNLESS OTHERWISE AGREED IN THIS CONTRACT, IN NO EVENT WILL CONTRACTOR BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. THIS LIMITATION WILL APPLY REGARDLESS OF WHETHER CONTRACTOR HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE FOREGOING LIMITATION MAY NOT APPLY.

36.21 Except to the extent expressly permitted in this Agreement or required by law, State shall not, directly or indirectly, or permit any third party to: (i) republish or redistribute any content or material (including any output generated by State) from the services, for any purpose other than the State's use of the services; (ii) make any alteration or modification to or translation of the services; (iii) reverse engineer, decompile, disassemble, or otherwise attempt to discern the source code, process flows, technical structure/architecture or other trade secrets of the services; (iv) resell, distribute or sublicense the services; (v) develop a product or service similar to or competitive with the Services having any functional attributes, visual expressions, or other features similar to those of the services; (vi) introduce or upload to the services any illegal content; or (vii) use the services (a) in a way prohibited by law, regulation, or governmental order or decree, (b) to violate any rights of others, (c) to try to gain unauthorized access to, test the vulnerability of, or disrupt the services or any other service, device, data, account, or network, (d) to distribute spam or malware, (e) in a way that could harm the services or impair anyone else's use of it, or (f) in a way intended to work around the services' technical limitations, recurring fees calculation, or usage limits. State hereby acknowledges that it is prohibited from using the services to store, transmit, or process personally identifiable information or personal data, criminal justice information, personal health information, or information otherwise governed by the Federal Bureau of Investigation's Criminal Justice Information Services Division and the Health Insurance Portability and Accountability Act.

37. Survival of Terms.

The following clauses survive the expiration or cancellation of this Contract: Indemnification; State Audits; Government Data Practices; Intellectual Property; Publicity and Endorsement; Governing Law, Jurisdiction, and Venue; and Data Disclosure. Any other Contract term that expressly states or by its nature shall survive, shall survive.

Exhibit B: Insurance Requirements

1. Notice to Contractor.

- 1.1 The Contractor is required to submit Certificates of Insurance acceptable to the State as evidence of insurance coverage requirements prior to commencing work under this Contract.
- 1.2 The Contractor shall not commence work under the contract until they have obtained all the insurance described below and the State has approved such insurance. Contractor shall maintain such insurance in force and effect throughout the term of this Contract, unless otherwise specified in this Contract
- 1.3 The failure of the Contractor to provide a Certificate of Insurance, for the policies required under this Contract or renewals thereof, or failure of the insurance company to notify the State of the cancellation of policies required under this Contract shall not constitute a waiver by the State to the Contractor to provide such insurance.
- 1.4 The State reserves the right to immediately terminate this Contract if the Contractor is not in compliance with the insurance requirements and retains all rights to pursue any legal remedies against the Contractor. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's Authorized Representative upon written request.
- 1.4.1 Because the Contractor's reseller(s) are independently owned and operated, and maintain their own insurance, the Contractor's reseller's insurance coverage must be evidenced by its own Certificate of Insurance. The Contractor's reseller's Certificate of Insurance must meet all the insurance requirements and limits set forth in the Contract.
- 1.4.2 The Contractor shall collect, review, approve, and maintain the applicable Certificates of Insurance, including but not limited to General Liability, Auto Liability, Umbrella, Workers' Compensation, and Garage keepers or Property of Others, for all Contractor's resellers that will be providing goods or services under this contract. The Contractor acknowledges compliance with this provision. The Contractor must provide copies of the dealers' insurance documentation to the State upon request.
- 1.4.3 If a claim is made against a Contractor's reseller, and the Contractor's reseller's insurance coverage did or does not cover the claim, the Contractor is responsible for the claim because the contract is with the Contractor. The Contractor must pay any uninsured claims out-of-pocket. The State may enforce the indemnity clause in the contract.

2. Notice to Insurer.

- 2.1 The Contractor's insurance company(ies) waives its right to assert the immunity of the State as a defense to any claims made under said insurance.
- 2.2 Insurance certificate holder should be addressed as follows:

State of Minnesota
50 Sherburne Avenue, Room 112
St. Paul, MN 55155

3. Additional Insurance Conditions. The following apply to the Contractor, or the Contractor's subcontractor:

- 3.1 Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract.

- 3.2 If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor agrees to notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State;
- 3.3 Contractor is responsible for payment of Contract related insurance premiums and deductibles;
- 3.4 If Contractor is self-insured, a Certificate of Self-Insurance must be attached;
- 3.5 Contractor's policy(ies) shall include legal defense fees in addition to its policy limits with the exception of professional liability.
- 3.6 Contractor's insurance companies must either (1) have an AM Best rating of A- (minus) and a Financial Size Category of VII or better, and be authorized to do business in the State of Minnesota or (2) be domiciled in the State of Minnesota and have a Certificate of Authority/Compliance from the Minnesota Department of Commerce if they are not rated by AM Best.
- 3.7 An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor's policy limits to satisfy the full policy limits required by the Contract.

4. Coverages. Contractor is required to maintain and furnish satisfactory evidence of the following insurance policies:

- 4.1 **Commercial General Liability Insurance.** Contractor is required to maintain insurance protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from claims for property damage, including loss of use which may arise from operations under the Contract whether the operations are by the Contractor or by a subcontractor or by anyone directly or indirectly employed by the Contractor under the contract. Insurance minimum limits are as follows:

\$2,000,000 – per occurrence

\$2,000,000 – annual aggregate

\$2,000,000 – annual aggregate – applying to Products/Completed Operations

The following coverages shall be included:

- Premises and Operations Bodily Injury and Property Damage
- Personal and Advertising Injury
- Blanket Contractual Liability
- Products and Completed Operations Liability
- Other; if applicable, please list _____
- **State of Minnesota named as an Additional Insured**, to the extent permitted by law

Evidence of Subcontractor insurance shall be filed with the Contractor.

- 4.2 **Workers' Compensation Insurance.** Statutory Compensation Coverage. Except as provided below, Contractor must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, Contractor will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State, including Coverage B, Employer's Liability. Insurance **minimum** limits are as follows:

\$100,000 – Bodily Injury by Disease per employee

\$500,000 – Bodily Injury by Disease aggregate

\$100,000 – Bodily Injury by Accident

If Minn. Stat. § 176.041 exempts Contractor from Workers' Compensation insurance or if the Contractor has no employees in the State, Contractor must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes Contractor from the Minnesota Workers' Compensation requirements.

If during the course of the contract the Contractor becomes eligible for Workers' Compensation, the Contractor must comply with the Workers' Compensation Insurance requirements herein and provide the State with a certificate of insurance.

4.3 Professional Liability, Errors, and Omissions. This policy will provide coverage for all claims the contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to Contractor's professional services required under the contract. Insurance **minimum** limits are as follows:

\$2,000,000 - per claim or event

\$2,000,000 - annual aggregate

Any deductible will be the sole responsibility of the Contractor and may not exceed \$50,000 without the written approval of the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources.

The retroactive or prior acts date of such coverage shall not be after the effective date of this Contract and Contractor shall maintain such insurance for a period of at least three (3) years, following completion of the work. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

Exhibit C: Specifications and Scope of Work

1.0 Radius Mapping

1.1 Product Specifications

Radius Emergency GIS Mapping Services

States, counties, and cities developing advanced cloud GIS services have a need to deliver location data securely and reliably to PSAPs for emergency calls alongside supplemental data call data and situational awareness data, available now and in the future.

When seconds count, Emergency Services need a single pane of glass to fuse all available integrated to the 9-1-1 Call Processing Equipment providing a full view of the emergency and the risk to first responders to route the right resources quickly and efficiently.

Radius 9-1-1 Call-Taking Map

Integrated with 9-1-1 Call Processing Equipment Radius connects directly with the Cloud Hosted GIS Services ensuring the most current and accurate data is used to determine the location of callers. Radius provides a statewide platform to deliver authoritative GIS data, commercially available GIS data, and supplemental call-taking data and supports legacy 9-1-1 networks, ESInet core services, and compatibility with advanced ESInet capabilities such as PDIF LO ingestion and plotting the event on the map seamlessly.

Radius Call-Taking Experience

Radius provides a seamless experience for call takers by automatically indexing the map to the location of the 9-1-1 call being answered to display the location of the caller, available supplemental data and situational awareness data quickly and automatically. When seconds matter Radius seamlessly fuses together all available information and modern communication tools in a single pane of glass.

Situational Awareness Data

- **Live traffic** integration, Waze Data, Waze Alerts
- **Satellite Imagery** from both commercial data partners such as Google, Esri, and Microsoft as well as authoritative aerial imagery via Esri integration.
- **Indoor floor plans** can be displayed automatically with caller location plotted directly on the map in either Esri GIS or Geo Tiff file formats for improved situation awareness.
- **CCTV Video feeds** are easily displayed by Esri interface that shows the location and one click streaming directly on the map in relation to 9-1-1 calls.
- **Esri native integration** tools enable agencies to quickly and easily integrate public and private Esri content such as trail maps, critical infrastructure locations, and resource status.

Advanced Mapping Tools

- **Forward/Reverse Geocoders** – unlimited number of geocoders can be configured and ranked enabling the use of both authoritative and commercial geocoders simultaneously.
- **Map Discrepancy Reporting** – users can quickly and easily flag map discrepancies which automatically route to GIS managers for review and validation.
- **Temporary Map Markups** – Users can identify and annotate areas and regions within the map specifying the time the temporary map markups should be visible to all users in the agency. This enables agencies to quickly communicate large-scale emergency events, public events such as parades, or disasters such as wildfires, and floods.

Supplemental Caller Location Data

- **Supplemental Mobile Device Location** Integration, allowing call-takers and Dispatchers to see supplemental location information from Apple EED and Google ELS including caller in motion.
- **Integration with ANI/ALI** via patented Emergency Data Gateway Device to capture and transmit CAD Spill data securely to the cloud.

- **Abandoned mobile call visibility** - Mobile Caller location is displayed on the map and signals queue even when the voice call is not connected.
- **Visualize misrouted calls** – Radius state-wide deployments enable each PSAP to see the location of mobile callers on the map and identify if that caller has been routed to an adjacent PSAP to see which PSAP answered the call.

Modern Communication Tools

- **The RapidLocate feature allows the caller** to send an SMS to a smartphone via Radius and return that phone’s exact latitude and longitude (mobile phone data connection required).
- **The RapidVideo feature allows the call taker to send an SMS to a smartphone** via Radius and turn the phone into a live, recorded video stream that plays back to the Dispatcher. It also returns the exact latitude and longitude.
- **Two-way SMS Texting** with native translation services built-in allows call-takers and dispatchers to communicate directly with callers outside of traditional text-to-9-1-1. The agency can configure preconfigured messages.

Vehicle Crash Telematics Data

- Correlated with ANI/ALI and Mobile Location Caller Data, Vehicle Telematics data is displayed as additional data which provides detailed location, vehicle propulsion data, condition, number of passengers, and, when available, calculated Injury Severity Prediction.

School Emergency Data

Radius provides an advanced, fully integrated, school and public building emergency workflow that allows agencies to connect and automatically correlate, authoritative GIS, caller location, Panic Button Data, Indoor Floor Plans, and mass communication tools.

- Audible alerts and displays are configurable enabling agencies the flexibility to configure emergency data per their SOPs.
- Radius integration to PSAP CPE ensures that Panic Button Callers are immediately identifiable, and their location is plotted on indoor floor plan data when available, saving valuable seconds in those most critical calls.
- Radius Modern Communication tools include the ability to text from 9-1-1 with translation and initiate streaming video services to see what the caller sees, providing critical situational awareness.

Esri Native, Public Safety Grade, Secure platform to ingest and correlate an agency’s authoritative GIS data with commercially available Esri GIS Services and Supplemental Data to provide a comprehensive situational awareness for every 9-1-1 call.

- Ability to integrate and natively display more than 20 base maps and feature layers, including ESRI, Google, Waze, TomTom, Azure Location Services, Bing, OpenStreetMap, and others.
- Deep ESRI integration with the ability to utilize agency REST service base maps and feature layer metadata natively within Radius.
- Esri Data can be deployed state-wide or by individual agencies ensuring the most relevant and critical data is available for the specific needs of the individual agency.
- In the event of a PSAP evacuation or outage, call takers can log into the Radius platform from any accessible internet-accessible computer and access data specific to their county and region.

The Power of the Cloud

- **Redundancy** – Supplemental mobile caller location (ELS & EED) data is delivered outside of the 911 network and correlated with 911 call data when received at the CPE. In the event of a 911 network failure, Mobile 9-1-1 callers will remain visible on the map and in the signals queue, enabling PSAPs to initiate contact with 9-1-1 callers even when their voice call is not routed to the PSAP.
- **Resiliency** – In the event of a PSAP evacuation or outage, call takers can log into the Radius platform from any accessible internet-accessible computer and access data specific to their county and region.

1.2 Radius Scope of Services

SaaS Product Offering

RapidDeploy products are offered as a Software as a Service (SaaS) which is always up to date and will grow and expand with the needs of the customer, providing a platform to deliver continuous improvements as new data, technology, and services become available to 9-1-1 networks and PSAPs.

- Hosted in the Microsoft Azure Cloud (Government Azure Cloud for US Government Agencies), the RapidDeploy platform is secure, redundant, resilient, and scalable for dynamic workloads.
- Every RapidDeploy customer is maintained on the same code base. As new features and functions are implemented, every customer will receive those upgrades as a part of their monthly SaaS subscription.
- System upgrades and new features and capabilities are also rolled out in real time without any loss of service.

Software as a Service Licensing

RapidDeploy offers cloud native Software as a Service (SaaS) products which are licensed based on the number of authorized seats. The Annual SaaS Subscription fee is calculated based on the number of licenses at the monthly license price for 12 months. Changes to the number of users or licenses required by the end customer will be reviewed on an annual basis and adjustments to the number of licenses or users will be made, if required.

SaaS Subscription Fees

The annual subscription for Eclipse software is due upon completion of the SaaS Milestone, as defined above, and execution of the SaaS Acceptance Form. RapidDeploy charges our SaaS subscription on an annual basis in advance. The subscription cost is due annually on the anniversary date from the date the SaaS was initially made available to the customer (SaaS Availability Milestone date).

Milestones, Acceptance Criteria

RapidDeploy standard SaaS Availability Milestone criteria are listed below and when completed represent the achievement of the milestone. These standard milestones are made a part of the agreement unless alternative milestone criteria is detailed in Exhibit D Quote.

The completion of delivery tasks, availability of features, capabilities, or services as detailed in the below milestone summary or milestone summary provided as part of Exhibit D represent acceptance and agreement.

Milestone Title	Acceptance Criteria	Charges / Fees
SaaS Availability	• Project Kickoff meeting conducted • Draft Project plan created and shared for review • Tenant(s) created and standard configurations applied (including RapidLocate, RapidVideo, and SMS Provider for Radius, as applicable) • Signals for Supplemental Device Location Service are enabled (Geofence is approved and configured) • System Administrators and/or Key Stakeholders provided access to tenants and RapidDeploy Learning Management System (LMS), as mutually deemed necessary	Annual SaaS Subscription Fee

Delivery of Radius – Required Customer Activities

The following activities are owned by the customer and RapidDeploy and must be completed as part of the initial requirements validation (discovery) phase:

1. Confirm client can provide ANI/ALI Spill outputs via configured Serial ports from the Call-Handling system or via IP if approved by RapidDeploy.
 - a. Once the connection is established between Client's call-handling system, the RapidDeploy implementation team will apply an initial parsing profile and will monitor parsing accuracy for up to 5 business days. If anomalies

are discovered, RapidDeploy will adjust the parsing profile as needed to address them and may, in some cases, engage the Client to investigate further to determine the adjustments that are needed. This DOES NOT constitute a dependency for Client SaaS Acceptance (per Section 5.2) and is considered normal course of deployment activities.

- b. In cases where Client has an integrated Text-to-911 solution in place and Text-to-911 calls are ingestible by the EDG device from the Client's call-handling system, additional custom parsing logic may be required. To properly ingest and plot Text-to-911 calls in Radius, the following data elements must be present in the ALI spill: Date/Time, Class of Service, Lat/Long, and Agent Position ID/#. RapidDeploy will work with the Client to confirm if this is the case and will collaborate with the customer and any third-party providers (e.g., CPE maintenance vendor) to determine what, if any, parsing logic adjustments are required. As this is considered non-standard for RapidDeploy implementations, this DOES NOT constitute a dependency for Client SaaS Acceptance.
2. Confirm Client approach to running RD Product on the floor (workstation access, internet, browser).
 - a. Radius is a powerful primary 9-1-1 call taking mapping application accessed by end users at the PSAP workstation on any chromium-based browser accessing the Azure Government Cloud. Chromium browsers can reside on a dedicated PC, CAD PC, CPE/CHE PC or Admin PC. While not a requirement, to provide an optimal user experience, Radius is best used on a dedicated monitor on the same computer as the call-taking application, which enables the user to easily copy and paste supplemental call data directly into call-taking and/or CAD systems and ensures every element of supplemental data is simultaneously displayed while the 911 call is being answered and handled.
3. Complete EDG Request for Information (RFI) form for all in-scope PSAPs, review and confirm ability to meet URL Whitelisting requirements (for web application operations) and IP Whitelisting and network connectivity requirements (for EDG installs)
4. Review and confirm ability to meet Hardware and Network specifications to support operations of RD products within Client environment.
5. Review and confirm technical approach for GIS data/service creation and management and ability to publish and host desired GIS services as ESRI REST services, (including determining if 3rd party is required) per RapidDeploy GIS Data Requirements.
6. Planned Client Upgrades – Document Client's planned upgrades to CHE/CPE equipment with vendors, versions, and timelines which may impact overall Project timelines.

Following the completion of the Requirements Validation Phase, RapidDeploy and Client will mutually agree on a Project Plan (Schedule), a Formal Project Kickoff Date, any updates to this Statement of Work, and Estimated Onboarding Completion Date. Should discrepancies be discovered after Requirements Validation is completed during the course of the implementation effort, RapidDeploy reserves the right to adjust the Project Plan (Schedule) to accommodate any impacts that result from such discrepancies or new information that is discovered.

Customer acknowledges receipt of the following requirements documents and confirms adherence to the requirements outlined therein:

- RapidDeploy Radius Hardware Requirements
- RapidDeploy Radius Network & URL Whitelisting Requirements
- RapidDeploy EDG Interface Requirements
- RapidDeploy Radius GIS Data Requirements

Integration to Call Handling / Call Processing Equipment

Radius utilizes RapidDeploy's Emergency Data Gateway (EDG) device which directly connects to a PSAP's on-premise or hosted Call Handling Equipment, enabling RapidDeploy products to retrieve the network location of 911 calls (ALI Spill) directly from the 9-1-1 Call Handling Equipment and display them on the Radius map. The EDG device integrates with Call Handling Equipment in one of two ways:

- CAD spill port using a serial cable connection
- IP-based network ingestion via ENTRA solution or TCP listener
- It is mutually understood that the following services will be provided by the customer, prime contractor, or third party and are out of scope for RapidDeploy:

- Installation of EDG device(s)
- Connectivity for EDG device(s)
- Field Service and Support for EDG device(s)

CHE Changes

RapidDeploy will integrate with the customer's existing Call Processing Equipment (CPE). RapidDeploy requires 1 month advance notice of any CPE changes, such as a migration to a new vendor, migration to a new version, and changes to ALI spill format. Failure to provide notice may result in temporary unavailability of the product for use.

Training

RapidDeploy's best-practice is to tailor the training program using RapidDeploy provided training and learning resources, with end-user training being driven by our clients.

Training activities for the Project are defined as follows:

- **Training Approach and Plan**

At the appropriate time during the project, RapidDeploy will conduct a Training Kick-off with the Client to define scope of training needs, led by the Client's assigned Customer Success Manager (CSM). This will include defining the delivery method(s), target audiences, and any additional relevant information to promote successful training of Client stakeholders and end users. The agreed-upon approach for Training will be documented and shared with Client stakeholders via email.

Unless otherwise specified, all training will be provided via the RapidDeploy Academy online Learning Management System (LMS), an on-demand training portal available 24/7/365. Should in-person training, live webinar training sessions, and/or a significant number of "Office Hours" sessions be requested by the Client, the RapidDeploy team will work with the Client to agree on an approach, which will be documented and reviewed. There may be an additional charge required if in-person and/or live webinar training sessions are desired by the Client.

- **Radius System Administrators Training**

System Administrators will be given access to Radius System Admin training modules in the RapidDeploy Academy. The primary audience for these training modules is PSAP training staff and/or supervisors who will then be able to enroll and direct the attendance of PSAP end users.

- **Radius End-User Training**

Radius End-User training modules are tailored to front line PSAP personnel and administered at a self-directed pace while seated at a console. System Administrators/Supervisors will be responsible for monitoring completion of the RapidDeploy Academy curriculum by the end users. Once complete, end users will receive a certificate.

- **"Office Hours" Live Training Sessions**

If requested and agreed, RapidDeploy will schedule and conduct a live, instructor-led webinar session to answer questions and provide in-depth review of specific application functionality, as requested by the Client. The RapidDeploy Customer Success Manager will work with Client to determine the quantity and timing of this session(s) based on need and availability of RapidDeploy staff.

In-depth training videos and training guides will also be made available to all PSAP end users via the Help Center, which can be accessed directly from the Support Portal within the RapidDeploy Radius application.

Radius SaaS Operation – Customer Success

Customer Success (CS)

RapidDeploy's Customer Success (CS) team works with all customers post-onboarding to drive on-going satisfaction and promote objective attainment across stakeholders. Our CS team's goal is to help every customer get the most from our products and services. As organizations grow, adjust policies and procedures and as products are updated, CS works with customers to support ongoing training activities via the RapidDeploy Academy and other channels, define and improve workflows using our products, and answer questions to drive alignment and overall success.

Feature and Enhancement Requests

Customers are our greatest source of inspiration. New feature and functionality requests are fielded by the assigned Customer Success Manager (CSM) and can also be submitted via the online help center or by emailing the RapidDeploy Support team. Requests are evaluated, prioritized, and planned with the help of our Customer Advisory Board (CAB), which comprises customers and industry leaders.

Product enhancements include workflow updates, reporting, administration, integrations, display, or user interface improvements. As a SaaS product, enhancements are included and made available to existing customers at no additional cost. New modules or additional product functionality may be developed, and these new modules may have an additional cost, new functionality are generally considered new functionality or capabilities that expand the use of the product, the types of users or the role of the users.

Vulnerability Risk Assessments

RapidDeploy completes external vulnerability and risk assessments with both third-party organization and automated security and vulnerability services. Vulnerabilities are categorized by severity and risk and added as planned software updates or critical software patches.

Platform Upgrades, New Releases

Through our SaaS delivery model, we maintain a single and unified codebase for all our customers with new features and capabilities feature flagged for activation upon user acceptance. Upgrades and new features are deployed on a scheduled and ongoing basis, in collaboration with Client and local stakeholders. If a new feature is not desired for Client or any of the PSAPs, the flag for the feature can be set to disable rather than executing a roll back of code. Each formal release is based on versioned components—each of which are rolled individually back if deemed necessary.

Critical Software Patch Release Process (HOT FIX)

RapidDeploy at its discretion may choose to complete a critical software patch or update outside of the normal release schedule when a vulnerability or software error presents a significant risk to customer operations.

Radius Terms of Use

Use of the Services

Client may use the Services only: (i) during the Subscription Term; (ii) for Client's internal business purposes; and (iii) in accordance with this Agreement and the Documentation. Client shall notify RapidDeploy of each billing metric added for purposes of using the Services. Client may only use the Product(s) it selects, and any further and future products, services, features, or functionalities may be requested from RapidDeploy and additional fees and charges may apply. On or after the Effective Date (as referenced in the relevant Order Form), RapidDeploy shall create an Account for Client to access the Services and shall provide Login Credentials to Client for that Account. To use the Services, Client must register and set up an authorized Account with Login Credentials. Client is responsible for any use of the Services that occurs under its Login Credentials, and Client is responsible for its Users' compliance with this Agreement. If Client becomes aware of any User's violation of this Agreement, Client shall promptly terminate that User's access and use of the Services.

Restrictions

To the extent expressly permitted in this Agreement or required by law, Client shall not, directly or indirectly, or permit any third party to: (i) republish or redistribute any content or material (including any output generated by Client) from the Services; (ii) make any alteration or modification to or translation of the Services; (iii) reverse engineer, decompile, disassemble, or otherwise attempt to discern the source code, process flows, technical structure/architecture or other trade secrets of the Services; (iv) resell, distribute or sublicense the Services; (v) develop a product or service similar to or competitive with the Services having any functional attributes, visual expressions, or other features similar to those of the Services; (vi) introduce or upload to the Services any Prohibited Content; or (vii) use the Services (a) in a way prohibited by law, regulation, or governmental order or decree, (b) to violate any rights of others, (c) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Services or any other service, device, data, account, or network, (d) to distribute spam or malware, (e) in a way that could harm the Services or impair anyone else's use of it, or (f) in a way intended to work around the Services' technical limitations, recurring fees calculation, or usage limits.

Ownership of the Services

RapidDeploy and its suppliers own and retain all right, title, and interest in and to the Services and any related RapidDeploy software, including all improvements, enhancements, modifications, and derivative works of them, and all Intellectual Property Rights in all of them. This includes any Analytics Data. Client's rights to use the Services are limited to those expressly granted in this Agreement. No other rights with respect to the Services, any related RapidDeploy software, or any related Intellectual Property Rights are implied.

Ownership of Content

Client and its Users retain all right, title and interest in and to any Client Content and all Intellectual Property Rights in the Client Content. Client's rights to access and use Client Content via the Services are limited to those expressly granted in this Agreement. Client hereby grants RapidDeploy a worldwide, non-exclusive, transferable, sublicensable, royalty-free, fully paid license to use the Client Content as necessary to provide the Services to Client under this Agreement and in accordance with its rights and obligations under this Agreement. Client Content will be returned to Client in a format reasonably determined by RapidDeploy upon written request following the expiration or termination of this Agreement.

Other Emergency Communications Service Provider Authorization

Client hereby authorizes RapidDeploy to provide "other emergency communications services" pursuant to 47 U.S.C. § 615b. These services include, but are not limited to, acquiring and transmitting Apple End-User EED Data, Google Android End-User ELS Data, and supplemental data from other sources to Client for the purpose of assisting in an emergency. Client acknowledges and agrees that RapidDeploy is and shall be an "other emergency communications service provider" in accordance with U.S. Code Title 47., Chapter 5., Subchapter VI., 615b and shall be subject to the immunities and other protections from liability set forth in U.S. Code Title 47., Chapter 5., Subchapter VI., 615b.

Data Security and Privacy

The terms and conditions that govern the parties' respective rights and obligations arising from and relating to data protection and data privacy are set forth in **Exhibit A** to this Agreement (the "**Data Protection Addendum**").

Support and Service Level Agreement

RapidDeploy shall provide Support in respect of the Services during the Subscription Term in accordance with Service Level Agreement as defined by CONTRACT FOR SERVICES C-585-23-002 Exhibit C. RapidDeploy shall use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week.

Third Party Content

As part of Client's use of the Services, Client may receive access to Third Party Content or sensitive Third-Party Content that is only accessible with the use of digital certificates. Client is responsible for complying with, and causing its Users to comply with, any terms that may be presented to Client when Client accesses that Third Party Content. RapidDeploy will determine in its sole discretion whether to (i) obtain digital certificates on Client's behalf and assign or transfer such certificates to Client, or (ii) require Client to obtain digital certificates itself. In the event RapidDeploy obtains digital certificates on behalf of Client and assigns or transfers those digital certificates to Client, Client will be responsible for complying with, and causing its Users to comply with, any terms and conditions presented by the provider of such digital certificates, and may be required to enter into a separate agreement with the provider of such digital certificates as a condition of accessing sensitive Third Party Content. Third Party Content is available "AS IS" without indemnification, support (unless otherwise specified), or warranty or condition of any kind. RapidDeploy, any provider of Third Party Content, and any provider of digital certificates necessary to access sensitive Third Party Content may suspend or terminate provision of any Third Party Content at any time, and that suspension or termination will not be deemed a material, detrimental change or a breach of this Agreement.

Third-Party Interfaces

Generally, RapidDeploy does not charge our clients one-time implementation charges for platform interfaces on the presumption that these will be delivered in a standardized and configurable manner and available to all RapidDeploy Clients.

It is mutually understood that Client may need to provision separately with existing third-party providers for accessing and activating direct connection from RapidDeploy's platform to third-party paid-for services. Client will provide those credentials to RapidDeploy to connect and integrate with such services.

2.0 Eclipse Analytics

Eclipse Analytics is RapidDeploy's cutting edge analytics platform that ingests your phone system (Call Data Record/CDR) into the cloud and generates unique insights and reports, including predictive and prescriptive analytics. The solutions are built on Microsoft Power BI and can be deployed alongside the agency's current 9-1-1 system. Eclipse Analytics goes above and beyond the standard PSAP reporting capabilities by offering a powerful, easy-to-use data discovery platform that assists PSAPs in addressing challenges such as workforce management and staffing or the lack of quality insights into call volumes and call transfers.

2.1 Eclipse Product Specifications

The following highlights the key capabilities and differentiators with Eclipse Analytics:

- Natural Language Query – access data quicker and more efficiently
- Staffing Analytics and Planning – make data-driven staffing decisions
- Call Detail Search – review the data behind every call
- Standard Reports Suite – easy access to frequently needed information
- Automated Report Scheduling and Electronic Delivery – get the information in your inbox
- Self-Service Analytical Reports – get quick answers to questions
- Interactive and Drillable Analytics – dive deeper for more information

Increase Understanding and Awareness of PSAP Performance

- User-friendly, flexible reporting with the ability to view key PSAP metrics, including Answer Time, Hold Time, Process Time, Talk Time, Answer Time Compliance to Standard, Abandoned Calls, and Transfer Calls
- Visualize individual performance metrics for a call taker
- Understand different variables that affect the overall time to process an incoming call
- Ability to explore data in depth

Call Reports

- Voice and General Text report by ESN, Trunk, PSAP, Shift, Call Taker, Position, Class of Service, and Time Period
- Complete call history from beginning to end
- Data export capabilities
- Search by call taker, address, date, or phone number

Natural Language Query

- Allows the user to easily create new reports by typing in what they want to see and how they want to see it, like internet search engines
- Eliminate the need for hundreds of standard canned reports with the use of on-demand reports
- No programming skills required

Staffing Forecast

- Visualize volume trends and optimize staffing levels easily
- Model based on call volume variations, changes to answer time goals, etc.
- Forecast call compliance to meet NENA or state requirements
- Reduce telecommunicator burnout by anticipating demand

Technical Requirements

- Procurement and installation of RapidDeploy approved web browser is out of scope for RapidDeploy.
- Internet connectivity to access the Eclipse platform is out of scope for RapidDeploy.
- Customer will provide necessary workstation hardware required to run the Eclipse web application at all PSAPs.
- EDG installations will require URL Whitelisting and IP Whitelisting.
- Features and Reports might not be available to all Client or Client locations. CPE/CHE deployment types and whether RapidDeploy can reliably and consistently get data will affect the availability of any feature at one or all Client locations. In order to deliver the intended behavior for each report, the required attributes listed for each report will need to be provided by the CDR/i3 feed. Some reports, filters, and features will be unavailable in the event not all required attributes are available. For clarity, Client must have Integrated Text-to-9-1-1 provided in the CDR or i3 logging feed to leverage for features and reports.
- All data in Eclipse is retained for 5 years unless otherwise required by applicable law, rule, regulation, or the terms and conditions of Client's contract with RapidDeploy.

2.2 Eclipse Scope of Services

SaaS Product Offering

RapidDeploy products are offered as a Software as a Service (SaaS) which is always up to date and will grow and expand with the needs of the customer, providing a platform to deliver continuous improvements as new data, technology, and services become available to 9-1-1 networks and PSAPs.

- Hosted in the Microsoft Azure Cloud (Government Azure Cloud for US Government Agencies), the RapidDeploy platform is secure, redundant, resilient, and scalable for dynamic workloads.
- Every RapidDeploy customer is maintained on the same code base. As new features and functions are implemented, every customer will receive those upgrades as a part of their monthly SaaS subscription.
- System upgrades and new features and capabilities are also rolled out in real time without any loss of service.

Software as a Service Licensing

RapidDeploy offers cloud native Software as a Service (SaaS) products which are licensed based on the number of authorized seats whose 911 and admin call taking activities data is recorded. The Annual SaaS Subscription fee is calculated based on the number of licenses at the monthly license price for 12 months. Changes to the number of users or licenses required by the end customer will be reviewed on an annual basis and adjustments to the number of licenses or users.

SaaS Subscription Fees

The annual subscription for Eclipse software is due upon completion of the SaaS Milestone, as defined above, and execution of the SaaS Acceptance Form. RapidDeploy charges our SaaS subscription on an annual basis in advance. The subscription cost is due annually on the anniversary date from the date the SaaS was initially made available to the customer (SaaS Availability Milestone date).

Milestones, Acceptance Criteria

RapidDeploy shall present SaaS Acceptance Form to Client for signature upon completion of the SaaS Availability Milestone. RapidDeploy standard SaaS Availability Milestone criteria are listed below and when completed represent the achievement of the milestone. These standard milestones are made a part of the agreement unless alternative milestone criteria is detailed in Exhibit D Quote.

The completion of delivery tasks, availability of features, capabilities, or services as detailed in the below milestone summary or milestone summary provided as part of Exhibit D represent acceptance and agreement.

Milestone Title	Acceptance Criteria	Charges / Fees
SaaS Availability	• Project Kickoff meeting conducted • Draft Project plan created and shared for review • Tenant(s) created and standard configurations applied • Customer System Administrators and/or Key Stakeholders provided access to tenants and RapidDeploy Learning Management System (LMS), as mutually deemed necessary • EDG Device(s) installed and fully operational (CPE events and/or CDR data processing, as applicable)	Annual SaaS Subscription Fee

Delivery of Eclipse – Required Customer Activities

The following activities are owned by the customer and must be completed as part of the initial requirements validation (discovery) phase:

- Confirm Customer can provide Call CDR (Call Detail Record) or i3 Event Log outputs via configured Serial ports from the Call Handling system or via IP if approved by RapidDeploy.
- Confirm Customer approach to running RD Product on the floor (workstation access, internet, browser).
- Complete EDG Request for Information (RFI) Form for all in- scope PSAPs, review and confirm ability to meet URL Whitelisting requirements (for web application operations) and IP Whitelisting and network connectivity requirements (for EDG installs).
- Review and confirm ability to meet Hardware and Network specifications (incl. bandwidth requirements) to support operations of RD products within Customer environment (control room and mobile).
- Planned Customer Upgrades (if applicable)– Document Customer’s planned upgrades to CHE/CPE equipment with vendors, versions, and timelines which may impact overall Project timelines.

Following the completion of the Requirements Validation Phase, RapidDeploy and Client will mutually agree on a Project Plan (Schedule), a Formal Project Kickoff Date, any updates to this Statement of Work, and Estimated Onboarding Completion Date. Should discrepancies be discovered after Requirements Validation is completed during the course of the implementation effort, RapidDeploy reserves the right to adjust the Project Plan (Schedule) to accommodate any impacts that result from such discrepancies or new information that is discovered.

Note: A Radius tenant will be created and configured for each in-scope PSAP as part of the project deployment. This is required to enable the capture of additional ALI data updates as part of call data ingestion. RapidDeploy will also configure Supplemental Device Location Services, using the in-scope PSAP geofence boundary. The Radius tenant will not be accessible to Client and will only be used by RapidDeploy unless a contract amendment is executed to add Radius to the subscription contract.

Customer acknowledges receipt of the following requirements documents and confirms adherence to the requirements outlined therein:

- RapidDeploy Eclipse Hardware Requirements
- RapidDeploy Eclipse Network & URL Whitelisting Requirements
- RapidDeploy EDG Interface Requirements

Integration to Call Handling / Call Processing Equipment

It is mutually understood that the following services will be provided by the customer, prime contractor, or third party and are out of scope for RapidDeploy:

- Installation of EDG device(s)
- Connectivity for EDG device(s)
- Field Service and Support for EDG device(s)

Data Retention and CHE Changes

RapidDeploy will integrate with the customer's existing Call Processing Equipment (CPE). RapidDeploy requires 2 months advance notice of any CPE changes, such as a migration to a new vendor, migration to a new version, and migration from traditional CDR to an i3 event logger. Failure to provide notice may result in lost data. Recovery of data or re-onboarding of a new CPE may require additional services to be quoted at the time of notice.

For customers who would like to extend their data retention beyond 5 years, an additional annual fee will be applied based on the overall call volume, for each year up to 10 years. Eclipse will begin aggregating data when the integration with the customer's existing CPE is complete. Uploading historical CDR data is possible to get jump-started with Eclipse, but also presents an additional onboarding effort. Upload requests will be evaluated for feasibility and a one-time fee may be applied based on the estimated effort and call volume of data being uploaded.

Training

RapidDeploy's best-practice is to tailor the training program using RapidDeploy provided training and learning resources, with end-user training being driven by our clients (i.e., "Train-the-Trainer"). Training activities for the Project are defined as follows:

Training Approach and Plan

At the appropriate time during the project, RapidDeploy will conduct a Training Kick-off with the Client to define scope of training needs, led by the Client's assigned Customer Success Manager (CSM). This will include defining the delivery method(s), target audiences, and any additional relevant information to promote successful training of Client stakeholders and end users. The agreed-upon approach for Training will be documented and shared with Client stakeholders via email. Unless otherwise specified, all training will be provided via the RapidDeploy Academy online Learning Management System (LMS), an on-demand training portal available 24/7/365. Should in person training, live webinar training sessions, and/or a significant number of "Office Hours" sessions be requested by the Client, the RapidDeploy team will work with the Client to agree on an approach, which will be documented and reviewed. There may be an additional charge required if in-person and/or live webinar training sessions are desired by the Client.

- **System Administrators Training**

System Administrators will be given access to Eclipse System Admin and Eclipse End User training modules in the RapidDeploy Academy once PSAP-specific data readiness activities have been completed. The primary audience for these training modules is PSAP training staff and/or supervisors. System Admins will then be able to enroll and direct the attendance of PSAP end users, who should be assigned the End User training module only, as appropriate.

- **End-User Training**

End-user training modules are tailored to PSAP personnel and administered at a self-directed pace while seated at a console. System Administrators/Supervisors will be responsible for monitoring completion of the RapidDeploy Academy curriculum by the end users. Once complete, end user will receive a certificate.

Additional training videos and training guides will also be made available to all PSAP end users via the Help Center, which can be accessed directly from the Support Portal within the RapidDeploy Eclipse application.

SaaS Operation - Customer Success

RapidDeploy's Customer Success (CS) team works with all customers post-onboarding to drive on-going satisfaction and promote objective attainment across involved stakeholders. Our CS team's goal is to help every customer get the most from our products and services. As organizations grow, adjust policies and procedures and as products are updated, CS works with customers to support on-going training activities via the RapidDeploy Academy and other channels, define and improve workflows using our products, and answer questions to drive alignment and overall success.

Feature and Enhancement Requests

Customers are our greatest source of inspiration. New feature and functionality requests are fielded by the assigned Customer Success Manager (CSM) and can also be submitted via the online help center or by emailing the RapidDeploy Support team. Requests are evaluated, prioritized, and planned with the help of our Customer Advisory Board (CAB), which is comprised of both customers and industry leaders.

Product enhancements include updates to workflows, reporting, administration, integrations, display, or user interface improvements. As a SaaS product, enhancements are included and made available to existing customers at no additional cost. New modules or additional product functionality may be developed, and these new modules may have an additional cost, new functionality are generally considered new functionality or capabilities that expand the use of the product, the types of users or the role of the users.

Vulnerability Risk Assessments

RapidDeploy completes external vulnerability and risk assessments with both third-party organization and automated security and vulnerability services. Vulnerabilities are categorized by severity and risk and added as planned software updates or critical software patches.

Platform Upgrades, New Releases

Through our SaaS delivery model, we maintain a single and unified codebase for all our customers with new features and capabilities feature flagged for activation upon user acceptance. Upgrades and new features are deployed on a scheduled and ongoing basis, in collaboration with Client and local stakeholders. If a new feature is not desired for Client or any of the PSAPs, the flag for the feature can be set to disable rather than executing a roll back of code. Each formal release is based on versioned components—each of which are rolled individually back if deemed necessary.

Critical Software Patch Release Process (HOT FIX)

RapidDeploy at its discretion may choose to complete a critical software patch or update outside of the normal release schedule when a vulnerability or software error presents a significant risk to customer operations.

2.3 Eclipse Terms of Use

Use of the Services

Client may use the Services only: (i) during the Subscription Term; (ii) for Client's internal business purposes; and (iii) in accordance with this Agreement and the Documentation. Client shall notify RapidDeploy of each billing metric added for purposes of using the Services. Client may only use the Product(s) it selects, and any further and future products, services, features, or functionalities may be requested from RapidDeploy and additional fees and charges may apply. On or after the Effective Date (as referenced in the relevant Order Form), RapidDeploy shall create an Account for Client to access the Services and shall provide Login Credentials to Client for that Account. To use the Services, Client must register and set up an authorized Account with Login Credentials. Client is responsible for any use of the Services that occurs under its Login Credentials, and Client is responsible for its Users' compliance with this Agreement. If Client becomes aware of any User's violation of this Agreement, Client shall promptly terminate that User's access and use of the Services.

Restrictions

To the extent expressly permitted in this Agreement or required by law, Client shall not, directly or indirectly, or permit any third party to: (i) republish or redistribute any content or material (including any output generated by Client) from the Services; (ii) make any alteration or modification to or translation of the Services; (iii) reverse engineer, decompile, disassemble, or otherwise attempt to discern the source code, process flows, technical structure/architecture or other trade secrets of the Services; (iv) resell, distribute or sublicense the Services; (v) develop a product or service similar to or competitive with the Services having any functional attributes, visual expressions, or other features similar to those of the Services; (vi) introduce or upload to the Services any Prohibited Content; or (vii) use the Services (a) in a way prohibited by law, regulation, or governmental order or decree, (b) to violate any rights of others, (c) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Services or any other service, device, data, account, or network, (d) to distribute spam or malware, (e) in a way that could harm the Services or impair anyone else's use of it, or (f) in a way intended to work around the Services' technical limitations, recurring fees calculation, or usage limits.

Ownership of the Services

RapidDeploy and its suppliers own and retain all right, title, and interest in and to the Services and any related RapidDeploy software, including all improvements, enhancements, modifications, and derivative works of them, and all Intellectual Property Rights in all of them. This includes any Analytics Data. Client's rights to use the Services are limited to those expressly granted in this Agreement. No other rights with respect to the Services, any related RapidDeploy software, or any related Intellectual Property Rights are implied.

Ownership of Content

Client and its Users retain all right, title and interest in and to any Client Content and all Intellectual Property Rights in the Client Content. Client's rights to access and use Client Content via the Services are limited to those expressly granted in this Agreement. Client hereby grants RapidDeploy a worldwide, non-exclusive, transferable, sublicensable, royalty-free, fully paid license to use the Client Content as necessary to provide the Services to Client under this Agreement and in accordance with its rights and obligations under this Agreement. Client Content will be returned to Client in a format reasonably determined by RapidDeploy upon written request following the expiration or termination of this Agreement.

3.0 Dedicated Customer Success

RapidDeploy offers dedicated customer success to work on behalf of The State in all PSAPs to facilitate training, best practices, coordinate meetings and support the States mission to bring NG9-1-1 tools to every PSAP. A dedicated person would be based in the State of MN and tasked with meeting onsite with PSAPs to complete training and education on services available to PSAPs. Travel and living expenses are included in the annual price.

4.0 Exchange LINK

RapidDeploy offers agencies using Radius the ability to display agency incident and resource location information alongside their existing 9-1-1 call data from a variety of sources by upgrading to Radius EXCHANGE LINK, a collaboration between RapidDeploy and Rave Mobile Safety provides interagency collaboration tools and workflow automation capabilities.

RADIUS EXCHANGE is an individually sold module that enhances Radius' capabilities by visualizing Incident and Responder Locations and collaboration tools to facilitate agency-to-agency data sharing, communication, and mutual aid requests.

RAVE LINK (formally Rave Aware) is a secure and interoperable solution for public safety agencies to speed response times by sharing CAD data, automating workflows, and more effectively collaborating across jurisdictions and on different CAD systems. Rave LINK provides data ingestion of Incidents and dynamic location of resources from an agency's CAD system, which can then be displayed within an agency's or an adjacent agency's Radius EXCHANGE Map or LIGHTNING Mobile Application. RAVE LINK gives 9-1-1 dispatchers, first responders, and relevant emergency service agencies the information they need to respond more effectively and cohesively to critical incidents.

4.1 Features & Functions

- **Cross Agency Visibility** - Sharing CAD data with neighboring organizations enables both jurisdictions to see events and updates in real time, allowing both teams to give a faster response, and increasing situational awareness across jurisdictions.
 - **CAD Incidents** - Ingest, normalize and distribute CAD Data with advanced filter by incident type to Radius users within your agency and permission based access by authorized neighboring agencies.
 - **CAD AVL** - Ingest, normalize and distribute CAD AVL Unit Location with advanced filter by Discipline and Unit Type, to Radius users within your agency and permission-based access by authorized neighboring agencies.
- **Proximity Alerts** - Key data from an ongoing event, including locations indicated on an interactive map, are used to automate critical notifications and quickly get the right information to the right people.
- **Complex Incident Management** - During complex situations that require coordinated effort across multiple agencies or jurisdictions, an incident can automatically trigger a dedicated collaborative event, assign tasks for your team to complete, and offer easy mechanisms for tracking progress and updates.
- **Notifications** via SMS, voice, email, or applications based on automated rules leveraging CAD incident data.

Rave shall provide the customer with a deployment and configuration point of contact on the Rave Services team. This person will provide you with necessary operational and technical documentation, answer questions, configure operational rules, and provide access to additional technical or operational personnel within Rave, as necessary.

- **Product Interfaces** - Configure and training for the operation of message template administrator interface for templated messages and automated rule-based sending by Rave Link to designated personnel.
- **Incident action plan** – Configure and train operation of administrator's interface for configuring event templates, tasks, assignments, and supplementary materials to guide your staff through manual or partly-manual processes.
- **Documentation and Tools** - Rave shall provide the necessary functional and technical documentation and tools necessary to facilitate deployment and train users on the Product Interfaces.

- (a) Interface functional user guides for necessary interfaces including Rave Alert and Rave Admin View.
- (b) Technical integration manuals explaining options for conveying CAD data to Rave.

- (c) Data mapping spreadsheets to facilitate mapping your data into Rave's standard data model to enable rule-writing and inter-agency data sharing.

4.3 Terms of Use - Acceptance of the Motorola Subscription Software Agreement is required for this option.

4.4 Customer Obligations

Rave Link provides powerful capabilities to optimize PSAP operations and reduce burdens on PSAP staff. To realize these benefits, an initial investment of effort is necessary to support the deployment and configuration of Rave Link. The efficiency of this deployment is dependent primarily on the PSAP's ability to provide relevant Information and Access to Data, via the involvement of necessary Personnel. Rave understands that the deployment of Rave Link is one of many important projects our customers are responsible for, and will work with you to deploy on a schedule realistic for your PSAP. However, experience has shown us that the customers who make a concerted effort to deploy as efficiently as possible derive the most benefit from the system.

The customer shall provide Rave two points of contact:

- 1) A Project Owner: This person shall be invested in the success of the project and responsible for ensuring the timely provision of necessary Information and Access to Data, as described below.
- 2) A Technical Lead: this person shall be responsible for the technical aspects of the product deployment.
- 3) The Project Owner and Technical Lead must possess information and expertise in the following areas, or else provide access to such people and ensure their cooperation:
 - PSAP Operations
 - CAD Administration
 - Information Technology (IT)

Information - PSAP Operations

- Operational Rules - The customer is responsible for defining all operational rules desired and indicating which message templates or incident action plan should be automatically invoked by Rave Link when the rule is satisfied. For example, "Send template "Notify Chief" when an event of type Structure Fire is detected within Fire District 1 geo-boundary".
- Geo-Boundaries - The customer is responsible for providing all geo-boundaries necessary for automated rules in a supported format. For example, if different fire chiefs are to be notified about the same type of events in different towns, a boundary file must be provided for each relevant area.
- Message Template Content & Message Targets
 1. The customer is responsible for managing the contact information for all people to be messaged via the system. Rave provides numerous ways to manage contact information manually or automatically - clearly documented in functional user guides.
 2. The customer is responsible for creating all templated messages that the customer desires Rave Link to send automatically when a Rule is invoked.
- Incident Action Plans, Steps, Resources, & Assignees - The customer is responsible for creating all guided incident action plans, adding checklist steps, creating assignments, and adding supplemental resources like documents.

- **Interagency Data Sharing**
 1. Rave Link can share data across agencies to improve situational awareness and inter-agency collaboration.
 2. The customer is responsible for establishing relationships with other PSAPs and agencies with which you wish to share data. The customer is responsible for specifying which specific event types and event data fields are permissible to share with which other entities.

Access to Data - CAD Administration

1. In order for Rave Link to function, the customer's CAD data fields must be mapped to Rave's NENA standards-based data model.
2. The customer is responsible for understanding your CAD system's data schema, agency-specific configurations, and how your PSAP uses CAD operationally such that you can indicate to Rave which fields and data values contain the data necessary for Rave Link to function.
3. If that knowledge is not available within the PSAP, the customer is responsible for working with your CAD company, consultants, or others to identify and indicate the necessary data fields.

Information Technology (IT)

1. The customer is responsible for providing secure network access to the PSAP in order to transport the necessary CAD data to Rave.
2. The customer is responsible for providing access to necessary CAD data via MSI connector and transport appliance, installed at Customer location, the customer makes the necessary data available to the tool through either:
 - a. XML or JSON files dropped in a location the tool reads from OR
 - b. creating a SQL Server view for the tool to read from.

5.0 Lightning Mobile App for First Responders

Powered by Radius Mapping, Lightning is a mobile application that delivers 911 data directly to first responders' devices, including smartphones and tablets. Lightning is built for first responders in the field and provides critical response capabilities and actionable intelligence that enhances situational awareness, supports unit safety, reduces response times, and improves emergency outcomes. Lightning extends the power of Radius Mapping beyond ECCs and into the field, supporting the secure and efficient sharing of data and critical information—all within an integrated 911 workflow.

Agency Licensing Program

RapidDeploy proposes an agency-wide license based on the total number of first responders within an agency. An Agency may be any entity with legal authority to direct or manage first responders, such as the individual county, city, ECC, Regional Council of Government, or State Agency. An Agency must have the legal right to authorize users to view confidential and sensitive 9-1-1 related data as a first responder in each or any of the roles of Law Enforcement, Emergency Medical Services, or Fire Service.

Agency licensing costs will be calculated based on the total number of first responders within the authorizing agency. We understand that deploying and utilizing Lightning within an agency is a matter of policy and strategy. Although not all first responders for a specific agency may use Lightning daily, the cost for an agency is based on the total number of first responders controlled by an Agency or ECC.

Lightning Mobile Product Specifications

Lightning is a unified communications mobile app built for first responders, powered by RapidDeploy's Radius Mapping solution. Lightning delivers 911 call data and critical information directly to the first responder's mobile device, reducing response times, improving outcomes, and supporting safety in the field. PSAPs and ECCs leveraging Radius Mapping can automatically send call data to first responders, ensuring they get the information they need as quickly as possible.

9-1-1 Caller Location

- Map-based view of active 9-1-1 calls and Radius Signals enables first responders to visualize nearby caller locations and access critical call data powered by Radius.
- Route to 9-1-1 Call Location: Select a 9-1-1 Call Location and utilize integrations with Apple Maps, Google Maps, or Waze for turn-by-turn directions.
- Supplemental Call Data: Field access to supplemental call data such as Apple ELS and Google EED, including the location of callers in motion.
- 9-1-1 Call Notifications: First responders automatically receive a notification when a 9-1-1 call is answered by the PSAP within proximity of the Lightning app user.

Situational Awareness for the Field

- Lightning displays Radius Signals with additional data, including Car Crash Signals and Panic Button Signals.
- Lightning enables first responders to join RapidVideo calls initiated by the PSAP, connecting them directly with citizens.
- Responders can access and view the text exchanges between the 911 call center and the caller during an emergency call.

Responder Location

- Lightning provides real-time location visualization of first responders in the field.
- Lightning pinpoints the exact location of first responders using the mobile app, providing Radius Users with a real-time view of their location directly within Radius Mapping.
- First responders leveraging the mobile app will be able to visualize the proximity of nearby responders and navigate to them utilizing mobile applications for turn-by-turn directions such as Apple Maps, Google Maps, or Waze.

Esri Authoritative, Supplemental and Partner Data

- Agency Authoritative Address Data, Commercial Maps configured in the PSAP can be provisioned and visualized by first responders directly in Lightning.
- Partner data such as PulsePoint AED Locations, indoor floor plans, and CCTV camera feeds are accessible in Lightning.

Technical Requirements

- Activation and utilization of Lightning requires an active Radius mapping subscription for the PSAP administering the Lightning user access credentials.
- The mobile device should be GPS enabled (i.e. support location services).
- Android devices must have Google Play services enabled.
- Android or iOS Mobile Smartphone Devices with the latest OS updates with backward compatibility of up to two prior releases. Lightning users must maintain the most current available version and cannot operate a version of Lightning that is less than 2 prior revisions.

5.1 Lightning Scope of Services Feb 2024

SaaS Product Offering

RapidDeploy products are offered as a Software as a Service (SaaS) which is always up to date and will grow and expand with the needs of the state, providing a platform to deliver continuous improvements as new data, technology, and services become available to 9-1-1 networks and PSAPs.

- Hosted in the Microsoft Azure Cloud (Government Azure Cloud for US Government Agencies), the RapidDeploy platform is secure, redundant, resilient, and scalable for dynamic workloads.
- Every RapidDeploy customer is maintained on the same code base. As new features and functions are implemented, every customer will receive those upgrades as a part of their monthly SaaS subscription.
- System upgrades and new features and capabilities are also rolled out in real time without any loss of service.
- Feature Flags Product Strategy enables states and PSAPs to configure services and capabilities by state, region, or PSAP.

Software as a Service Licensing

RapidDeploy offers cloud native Software as a Service (SaaS) products which are licensed based on the number of end users, average concurrent users or total users in an agency. The Annual SaaS Subscription fee is calculated based on the number of licenses at the monthly license price for 12 months. Changes to the number of users or licenses required by the end customer will be reviewed on a yearly basis and adjustments to the number of licenses or users.

Non-Recurring Costs, Project Fees and Fee Schedule

Non-Recurring Costs are detailed in the Quote and payable due upon completion of Project Milestones in accordance with the milestone schedule.

Milestones, Acceptance Criteria

The subscription cost is due annually on the anniversary date from the date the SaaS was initially made available to the customer ("SaaS Availability Date" or "SaaS Availability Milestone").

SaaS Availability for Lightning is based on (a) the availability of the Lightning Mobile App made available for download via Android or iOS marketplaces, (b) the service being made available within Radius to provision Lightning Users. The date of SaaS availability will be the start of the annual performance period.

SaaS Subscription Fees

RapidDeploy is a Software as a Service (SaaS) platform, the annual subscription for RapidDeploy's software is due upon provisioning of the initial client environment(s). RapidDeploy charges our SaaS subscription on an annual basis in advance when the initial environment and infrastructure has been configured and made available to our clients (SaaS Availability Milestone). The subscription cost is due annually on the anniversary date from the date the SaaS was initially made available to the customer (SaaS Availability Milestone date).

Delivery of Lightning

- RapidDeploy's Delivery Team will work with Customer stakeholders to define and execute a deployment plan.
- RapidDeploy will configure the required feature flags to enable use of Lightning in conjunction with the in-scope Radius tenant(s), as required.
- Lightning will be made available for download from Apple and Android mobile application stores.
- Customer Radius Administrators will be granted access to and own the configuration of Lightning features and functions for field responders as well as Lightning-related features/functions within Radius.
- Customer Radius Administrators will manage Lightning user creation and assigning and management of user roles, rights, and data access.
- All Lightning and PSAP users will have access to Lightning articles and training material within the RapidDeploy Help Center. Lightning will also contain in-app guides and tutorials to assist users in operation of the application.
- Radius (PSAP) users will have access to the Lightning content within the RapidDeploy Help Center as well as Lightning-related content in the RapidDeploy Academy (online LMS).

Excluded from Scope of Services

The following are specifically not supplied by RapidDeploy but are functional requirements of the product:

- Supply, procurement, or deployment of mobile devices and maintenance and support of such mobile devices.
- Mobile data / cellular connectivity or related services, including support
- Any equipment (including mobile device) upgrade not identified in this proposal but required to run new or updated software.

Customer Support

Each customer agency (PSAP) will appoint an internal owner (or group of owners) for Lightning Mobile App management, who will develop policies, procedures and manage training and deployment of the Lightning Mobile Application. The Lightning Mobile App management person/team will work with an Agency's Radius Mapping Administrator to ensure the appropriate and approved Radius Data is configured and available in the Lightning Mobile Application.

Individual Lightning end-users (field responders) will be instructed to refer all questions on training, operation, and policy to their Agency's Lightning management contact, who will validate the Lightning end-user is operating the application correctly, work with the Radius Mapping Administrator to confirm the data is available in Radius and confirm if a product trouble ticket should be raised.

Post Deployment, Agency Lightning management contact(s) will open trouble tickets for the Lightning Mobile App with RapidDeploy Customer Support.

SaaS Operation - Customer Success

RapidDeploy's Customer Success (CS) team works with all customers post-onboarding to drive on-going satisfaction and promote objective attainment across involved stakeholders. Our CS team's goal is to help every customer get the most from our products and services. As organizations grow, adjust policies and procedures and as products are updated, CS works with customers to support on-going training activities via the RapidDeploy Academy and other channels, define and improve workflows using our products, and answer questions to drive alignment and overall success.

Feature and Enhancement Requests

Customers are our greatest source of inspiration. New feature and functionality requests are fielded by the assigned Customer Success Manager (CSM) and can also be submitted via the online help center or by emailing the RapidDeploy Support team. Requests are evaluated, prioritized, and planned with the help of our Customer Advisory Board (CAB), which is comprised of both customers and industry leaders.

Product enhancements include updates to workflows, reporting, administration, integrations, display, or user interface improvements. As a SaaS product, enhancements are included and made available to existing customers at no additional cost. New modules or additional product functionality may be developed, and these new modules may have an additional cost, new functionality are generally considered new functionality or capabilities that expand the use of the product, the types of users or the role of the users.

Vulnerability Risk Assessments

RapidDeploy completes external vulnerability and risk assessments with both third-party organization and automated security and vulnerability services. Vulnerabilities are categorized by severity and risk and added as planned software updates or critical software patches.

Platform Upgrades, New Releases.

Through our SaaS delivery model, we maintain a single and unified codebase for all our customers with new features and capabilities feature flagged for activation upon user acceptance. Upgrades and new features are deployed on a scheduled and ongoing basis, in collaboration with Client and local stakeholders. If a new feature is not desired for Client or any of the PSAPs, the flag for the feature can be set to disable rather than executing a roll back of code. Each formal release is based on versioned components—each of which are rolled individually back if deemed necessary.

Critical Software Patch Release Process (HOT FIX)

RapidDeploy at its discretion may choose to complete a critical software patch or update outside of the normal release schedule when a vulnerability or software error presents a significant risk to customer operations.

6.0 Motorola (Rave) Smart911

Smart911 offers a transformative advantage for 9-1-1 call takers and first responders in Minnesota, especially those already using the Radius platform. By integrating Smart911's detailed individual safety profiles into Radius, call takers gain immediate access to vital personal information during emergency calls. This integration significantly enhances the call takers' ability to understand the context of each emergency, allowing them to relay critical information to first responders en route. For first responders, having details like medical conditions, physical descriptions, and location-specific notes at their fingertips means they can tailor their response strategies even before arriving at the scene. This proactive approach is particularly beneficial in time-sensitive situations where every second counts. The integration into Radius streamlines the communication process, ensuring that crucial information flows seamlessly from the call taker to the first responders, thus facilitating a more efficient and effective emergency response.

Rave Facility data into the Radius platform provides unprecedented situational awareness for both 9-1-1 call takers and first responders in Minnesota. With its comprehensive building and facility information, this system has become an invaluable tool for emergency personnel. For call takers, access to Rave Facility data means they can quickly understand a location's layout and specific challenges, enabling them to guide first responders more effectively. They can inform responders about the best access points, potential hazards, and key structural details of the facilities involved. For first responders, this translates into a significant strategic advantage. Knowing the intricacies of a building's layout or the specifics of a facility's infrastructure allows them to plan their entry and operations more effectively, reducing the risks and potentially saving more lives. Integrating Radius enhances the coordination between call takers and first responders, ensuring that both parties comprehensively understand the emergency, leading to more efficient and safer resolutions.

6.1 Smart 911 Integration to Radius and Lightning

The integration of licensed Rave Smart911 data to Radius is free. Agencies with Smart911 licenses can visualize Smart911 People or Facilities Profiles, automatically displayed in Radius as additional data for the specific 9-1-1 call received, ensuring consistent real-time data delivery. Smart911 data is also available to First Responders via LIGHTNING Mobile Application.

6.2 Smart 911 Features & Functions

- **Smart911 Profiles** - Gives PSAPs and first responders access to a 9-1-1 caller's profile: family member info, photos, medical conditions, disabilities, exact addresses, even pet information, to make informed dispatch decisions.
- **Facilities** - Facilities create profiles containing floor plans, key holder, alarm, and Hazmat information, gate/access codes, points of contact, AEDs, and more. Profiles automatically display during 9-1-1 calls and are searchable by authorized users

6.3 Smart 911 Statement of Work

Rave 911 Suite Components

- **Smart911.com Citizen Registration Portal** - Hosted, secure website enabling an unlimited number of citizens to register and maintain their profile at no cost to them.

- **Rave Facility Registration Portal** - Rave Facility provides businesses, schools, healthcare centers, government or any other non-residential properties with a free, secure and convenient way to share critical information about their facility with 9-1-1 and other responders during an emergency, significantly improving emergency response.
- **Rave Dispatch View and First Responder View** - Hosted, secure online portal providing first responders and dispatchers access to subscriber account profiles for active cases based on user id, password and case ticket number (which is generated by Rave 911 Suite)
- **Rave Admin View** - Hosted, secure online portal providing administrative functions such as user management and reporting.

Rave's Responsibilities

- **Remote Deployment Services** - The following remote deployment steps will be performed to implement these components:
 - **Perform the necessary set up and configurations** to track citizen registrations and PSAP usage data for reporting purposes
 - **Set up and provide access information** for administrative accounts
- **Training and Support** - Provide unlimited, on-demand access to Rave Academy (Rave's online video-based training platform), product guides, 24x7 phone & email technical support, and sample SOPs, best practices and FAQ documents.
- **Marketing Services** - Online access to marketing best practices guides, Smart911 and Facilities public outreach materials including flyers, web graphics, social media graphics, and content for presentations, newsletters and emails. Access to the Rave Community Engagement Manager is also available.

Client Responsibilities

This project requires technical and operational support within the client environment as well as marketing support across the supported communities to ensure success. The following outlines expected functions to be performed in support of the Rave 911 Suite deployment:

- **Project Management** and Executive Support
- **Integration of information** available from Rave 911 Suite into the correct PSAP procedures and best practices as well as any training required to ensure proper implementation of those procedures
- **Support for the technical deployment** providing remote access for Rave Mobile Safety to be able to complete the installation of Rave 911 Server software and Rave Dispatch View workstation software.
- **Broad public awareness campaign** to ensure citizen adoption. Examples include inclusion of registration links on community websites; the inclusion of registration reminders in written communications with citizens; email marketing campaigns; and distribution of registration information through community channels such as schools, elderly centers, hearing disabled communities and libraries.

6.4 Smart 911 Terms of Use

- Acceptance of the Motorola Subscription Software Agreement is required for this option.

7.0 Skyline Video Sharing Platform

RapidDeploy offers additional services from Skyline Technology Solutions as a Subcontractor to provide a platform to manage closed-circuit camera networks and capability to visualize them in the mapping application

Skyline Technology Solutions, LLC (Skyline) has been delivering interoperable video sharing solutions for nearly 13 years to state and local government agencies. The original Skyline video sharing solution was developed from solving a significant customer pain point; the Maryland State Highway Administration (SHA) was unable to share video with any partner, even internally, without the high cost of leased circuits and proprietary, end of life equipment that represented little interoperability. Skyline resolved SHA's pain by developing our original video sharing product.

Today, Skyline's video sharing ecosystem is the industry leading video distribution solution for agencies across the country. Currently, Skyline provides statewide video sharing platforms for the Maryland Fusion Center, 17 State DOTs and their trusted public safety and first responder agency partners. Skyline streams over 50,000 cameras in North America, 24/7 to support customer operations, emergency response and public roadway awareness.

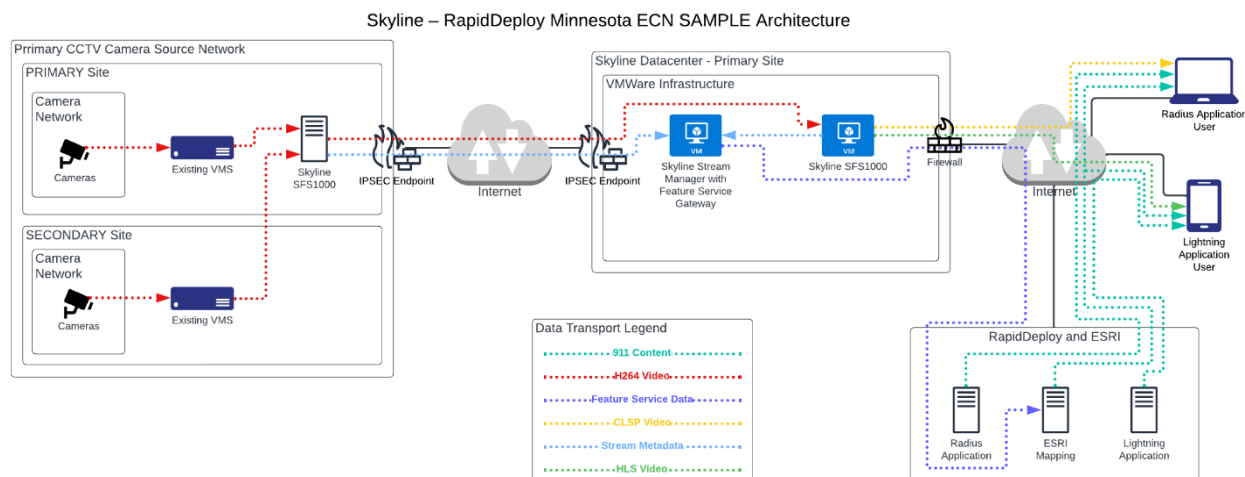
Implementing Skyline's Video Sharing Ecosystem in Minnesota to integrate with Radius and Lightning will bring enhanced situational awareness for emergency responders at in-office call taking positions as well as first responders in the field. Having access to Skyline's low latency, real-time streaming video in both Radius and Lightning will allow Minnesota public safety workers to execute on their critical responsibilities safer, faster, and more effectively.

Integration of closed-circuit camera streams into Radius and Lightning

Skyline will deliver to Minnesota ECN real-time streaming video into RapidDeploy's Radius application and Lightning mobile application. This real-time video will be available in the map view, providing mission critical info to 911 operators and to the mobile devices of those first responders in the field en-route and on-site. Getting live video from the area in and around a time critical event reduces the time to resolution and helps ensure safety of responders - saving lives.

Central to the Skyline video solution is our Stream Manager application: a central repository and an API endpoint for clients to acquire stream URL, metadata, and status information. This application synchronizes with our Video Streaming application (SFS1000) to facilitate the distribution of video streams to end users. Multiple SFS1000 instances can be deployed and configured to create specific security "zones," designated for *public* or *private* stream use cases. For Minnesota ECN, only a single security zone will be required for integration with RapidDeploy. From the Stream manager operators can manage streams on each SFS1000, edit pertinent metadata including camera latitude/longitude, route name, mile maker, jurisdiction, etc., and to set streams offline if necessary.

To support integration with RapidDeploy, the Stream Manager exports and continuously updates the metadata for every stream to Esri within a Feature Layer. RapidDeploy's Radius and Lightning applications leverage this Esri Feature Layer data to present camera location, metadata, and live video streaming alongside their 911 operator toolsets.



Skyline's video ecosystem has the flexibility to integrate video from multiple source organizations, spread across several sites and various networks. The diagram above depicts one source network with PRIMARY and SECONDARY sites shown (as typical as video sharing expands to multiple sites). The PRIMARY site is designated as the aggregate location to bring all video traffic together and send back to Skyline's datacenter over an encrypted transport tunnel.

Once the video is routed back to Skyline, we host the video for RapidDeploy on our video platform. The Stream Manager - Feature Service will publish the stream metadata to ESRI as a Feature Layer, providing stream metadata in Radius and Lighting, as described above. When users click on a camera, video data is streamed directly from the Skyline platform to their device. Since we host the video for consumers, additional client connections only impact bandwidth at our datacenter, not on the client network.

7.1 Skyline Scope of Integration

This is Indicative Scope and Pricing. Ultimate architecture and scope of work will be finalized upon site survey and specification sharing working sessions with the Minnesota ECN, initial camera source technical staff and Skyline's network engineering staff.

- Streaming video to be integrated into RapidDeploy Radius and RapidDeploy Lightning.
- Minimum camera count for initial deployment is 400 cams. There are no maximums, the camera inventory can grow indefinitely through the contract period.
- Initial scope will be Standard Quality streams. High Quality streams can be added at additional cost.
- Participating organizations will make video available to Skyline for the solution. Video provided will be H.264 baseline, 320x240 resolution, 192kbps, 15fps.
- Initial scope does not include transcoding. Transcoding is required to pull video from specific VMS's, change video encoding, or stream spec (resolution, framerate, bitrate), and is available at additional cost.
- 2-year initial contract engagement, with the option to extend up to an additional 72 months in increments determined by the state.

7.2 Skyline Assumptions

- Initial scope assumes Skyline's applications will reside on VMs on-site in Minnesota ECN and/or camera source providing agency (example: MnDOT or other). Hardware hosts, network hardware, and VMware compute will be provided by Minnesota ECN for any on-premises video platform components. NOTE: this is a sample architecture (as reflected in above diagram). Ultimate solution architecture to be determined upon collaboration with initial video sharing source.
 - Skyline will not be providing physical hardware in this scope.
 - Skyline can also accommodate hosting the applications in Skyline's datacenter; that may impact the scope.
- Minnesota ECN and partner agencies supplying video have an existing Video Management Systems (VMS) that manages their video cameras. Skyline proposes to interface with these VMS platforms.
 - VMS and VMS Management of cameras is not in scope of this response, although Skyline is happy to discuss additional services we can offer in this realm.
- Minnesota ECN has network access to video sources that is in alignment with their Cybersecurity policies and their partners' policies.
- An internet connection at the ECN customer site with access to this video platform will be made available with sufficient bandwidth to stream all video outbound to the Skyline datacenter to facilitate integration into Radius and Lightning.
- An IPSec endpoint tunnel configuration will be installed on existing Minnesota ECN networking equipment (firewall) in Minnesota with the remote help of Skyline network engineers.
- All network architecture and other integration assumptions will be confirmed during site survey and technical collaboration between Minnesota, RapidDeploy, and Skyline.
- Skyline engineers will be able to remotely access and monitor all Skyline applications existing on-site in Minnesota for the video platform.
- For the purposes of this proposal, Skyline capacity and pricing is based on a minimum of 400 video streams for this engagement.

- The Skyline datacenter will be the point of external presence for video hosting.
- Minnesota ECN has capability to host an Esri Feature Service Layer that will include links to Video sources and will be incorporated into Radius and Lightning.
- Video will be presented using Skyline's CLSP player, via links embedded in the Esri Feature Service.

7.3 Description of the Services

VSAAS Per Camera/Per Year includes: Streaming video to the internet with one security zone; Stream Manager portal, API service, Auto Offline, and ESRI feature map integration is included; Secure network link from customer OT network to Skyline VSAAS Data Center; Network bandwidth on the cloud side; Monitoring and management of remote VSAAS components on customer premises; Operations and maintenance of cloud environment

7.4 Billing Terms

- Deployment – Customer will provide signed Acceptance of the final solution prior to the solution being launched to Production. The solution will migrate into production only after acceptance and sign-off. Skyline will invoice for Deployment immediately upon Acceptance.
- Recurring Video as a Service – Skyline invoices quarterly, at the beginning of the respective quarter, for the recurring Video as a Service based upon the number of streams currently in the platform. Streams added to the platform are considered live in the month they are added and will be invoiced in the next quarterly invoice prorated to the month the streams were added.
- Video as a Service pricing is based on a 2-year initial contract engagement with the option to extend up to 72 months in increments determined by the state.

7.5 SKYLINE Pricing Assumptions

- Based upon standard quality streams (320 x 240 pix, 15 fps, 192kbps).
- High-quality streams may be added for additional cost.
- This pricing does not include any hardware costs. Video source agencies will provide network hardware to host the IPSec tunnel endpoint in Minnesota.
- This pricing does not include any costs related to circuits, bandwidth, or network devices located at Minnesota facilities to source the video to Skyline's Data Center.

8.0 CRG Mapping

Critical Response Group Inc. proposes a mapping solution developed by US Special Operation Forces and is now used by security teams and public safety professionals. Collaborative Response Graphics® (CRGs) are site-specific common operating pictures that enable better communication during an emergency. CRGs combine accurate floor plans, high-resolution imagery, emergency response pre-planning, and gridded overlays into one map. Critical Response Group builds CRGs and distributes them to local, county, state, and federal public safety agencies through various software applications like RapidDeploy. It also provides the necessary training to ensure full implementation.

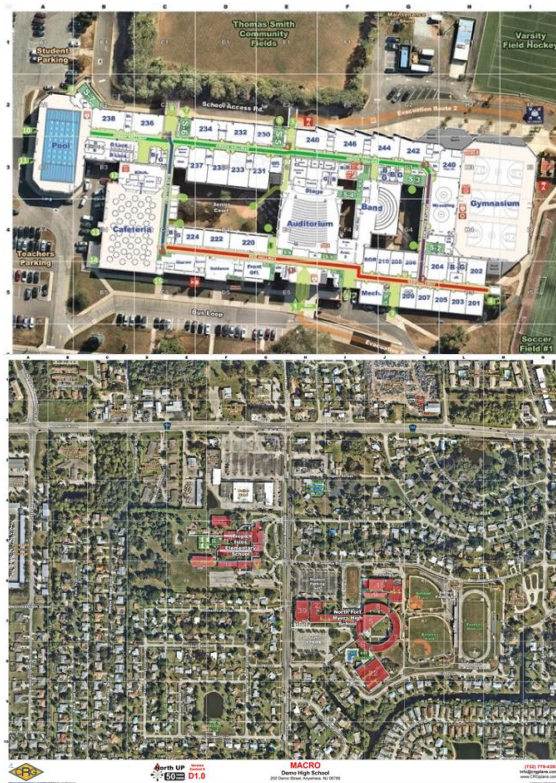
Schools Systems, Counties, Cities or Regions can leverage this purchasing agreement to contract with CRG individually or jointly for the mapping of indoor schools at the fixed price offered under this agreement. Volume discounts may be available at time of contracting.

Mapping of non-education facilities such as hospitals, government or public buildings will be quoted based on the square footage of the building and the number of buildings contracted.

8.1 Collaborative Response Graphics® (CRGs) are site-specific common operating pictures that enable better communication during an emergency. CRGs combine accurate floor plans, high resolution imagery, emergency response pre-planning, and gridded overlay into one map. Critical Response Group builds CRGs and distributes them to first responders through a variety of software applications and provides the necessary training to ensure full implementation.

1) **Micro CRGs small-scale)** are built for each floor of a facility, combining floor plans, a gridded overlay, and high-resolution imagery together into one map. Micro CRGs include site-specific details that a first responder needs to coordinate an emergency response inside a structure. This includes room labels, hallway names, external door/stairwell numbers, locations of hazards, key utility locations, security cameras, key boxes, AEDs, and trauma kits, and other pertinent information unique to a facility. Many schools utilize Micro CRGs to depict school reunification plans visually for both on-site and off-site reunification locations.

2) **MACRO CRGs (large-scale)** are built for a structure's overall campus or grounds. Macro CRGs combine a gridded overlay and (current) large-scale aerial imagery with accurate labeling for parking areas, athletic fields, surrounding roads, and neighboring properties. First responders and building administrators use a Macro CRG to coordinate crisis response outside a structure, including inner and outer security perimeters, ambulance staging areas, command posts, reunification areas, etc. Buildings that are contiguous to each other or are in very close proximity may share a Macro CRG. Pre-planned incident response information, like staging areas, command post locations, traffic control points etc., can also be depicted visually on the maps.



8.2 CRG Delivery

Building Collaborative Response Maps is typically a four-to-six-month process. The speed of completion principally depends on how fast Critical Response Group can gather initial floor plans, coordinate and schedule site visits, and gain final approval for publishing of each product.

Creation for Critical Response Mapping Content: For creation of Micro and Macro CRG mapping data, Critical Response Group assigns a Project Manager to complete the following steps ensure that CRG maps are accurate and accessible comprehensively to the entire public safety community.

Gathering Floor Plans: To begin the project, we require the best floor plans that the school currently has on file. On the rare occasion no floor plan exists, we may utilize scanners to map the interior building to generate an accurate two-dimensional floor plan. Because floor plans are stored in a multitude of disparate physical and digital formats, we utilize several proprietary work flows to accommodate any floor plan we receive, whether it is a scan of a rolled-up physical “blueprint” or a .dwg file from AutoCAD software.

- 1) **Proof Creation:** We create initial Micro and Macro proofs of the facility by combining baseline interior floor plans with high-resolution overhead imagery of the site.
- 2) **Site Walk-Through:** We conduct an on-site walk-through with an initial CRG proof to create an accurate map. Our on-site labeling process allows us to update or verify floor plan accuracy (both in the structure and labeling of buildings), capture site-specific terms used for locations at a facility and identify and label unique features for each structure.
- 3) **CRG Approval:** We update proofs based on data we collect during site visits and submit them to a site point-of-contact for feedback. First responders are also consulted for modifications and once we finalize proofs, building managers approve them for final publishing.
- 4) **Final Publishing:** We overlay a grid on each CRG so first responders can quickly and easily orient to any location. The CRG is geo-rectified through a proprietary process that allows us to save it in a variety of geo-spatially relevant industry file types, allowing each CRG to be uploaded as a distinct layer in disparate platforms. CRGs are currently published as GeoPDFs, PDFs, JPEGs, KMZ/KML, GeoTIFFs, MBTILES.

8.3 Critical Response Group Annual Maintenance SOW

School Mapping data must be accurate and accessible for the 911 community to effectively utilize during a 911 event. Therefore, Critical Response Group provides a maintenance plan after the first year if any necessary changes are needed. Critical Response Group offers a Maintenance Plan to its Clients as a service for an additional fee. Benefits of the plan to Clients are:

- Ensures that Collaborative Response Graphics distributed to first responders remain accurate, up-to-date depictions of your buildings and grounds.
- When changes to floor plans have occurred, CRG will perform an on-site walk-through and Collaborative Response Graphics will be updated to reflect the current layout of the school. This includes updating floor plans, room designations, and any other required labeling. If the exterior school grounds have changed, the background imagery of the Collaborative Response Graphics will be updated if new imagery is available from our providers. If necessary, we can provide drone imagery at an additional cost.
- Revised Collaborative Response Graphics are distributed to the school in digital format.
- Revised Collaborative Response Graphics are provided to the BAE Systems GXP program managers (where applicable) so that Collaborative Response Graphics can be made available to law enforcement officers on mobile devices.
- Revised Collaborative Response Graphics are distributed to local first responders (police, fire, EMS), at the direction of the Client.
- Revised Collaborative Response Graphics will be distributed to the client’s 911 call center / police dispatch point, at the direction of the Client.

8.4 Distribution of CRGs to Public Safety within Radius

CRGs are hosted in a cloud repository by CRG, accessed by ECCs, and visualized in a georeferenced format within the authoritative base map of a Radius ECC. Agencies or States with licenses can visualize CRGs automatically displayed in Radius as map features in proximity to the specific 9-1-1 call received, ensuring consistent delivery of real-time data. CRG data is also available to First Responders via LIGHTNING Mobile Application. The integration of Critical Response Graphics to Radius is offered as a no-cost integration.

- Calls are automatically plotted in Radius visualized on the CRG of a school.

- When an emergency call is received from a school with a CRG, a 911 operator can quickly reference location information on a CRG directly within Radius, allowing that operator to make faster decisions and communicate more effectively to dispatch first responders.

Exhibit D: Pricing

The following price schedule is hereby attached and incorporated into this agreement as Exhibit D.

Each individual service offering as defined in Exhibit C: Specifications, Duties, and Scope of Work is presented below and is offered based on the specific SOW as defined in Exhibit C including any required terms of use as defined in each service item in Exhibit C.

Each service may have Annual Software as a Service(SaaS) license fees and or Product Specific Non-Recurring Costs(NRC). The Pricing Model description indicates the specific definition of the license or cost metric used to calculate the fee.

Prices presented are for the initial contract term and will not increase during the initial term. Subsequent renewal term pricing will not increase more than the greater of: (a) the then-current year-to-year increase in the Consumer Price Index ("CPI"); or (b) five percent (5%).

CPV contract users need approval from MN ECN/DPS to purchase optional services.

Prepayment discounts are available for the payment of annual SaaS fees of 24 months or more.

Service	Product	Pricing Model	Example Unit / Qty	Unit / Qty Price	Annual SaaS Price	NRC
SOW Item 1.0	Radius Mapping	Avg Concurrent Call Taking Positions	338	\$ 130.50	\$ 529,308	
SOW Item 2.0	Eclipse Analytics SaaS	License calculated by the total number of authroized call taking positions for participating ECC	1	\$ 170	\$ 170	
	Eclipse Analytics	NRC Redundant EDG per CPE	1	\$ 2,300		\$ 2,300
SOW Item 3.0	Dedicated MN Customer Success	Annual fixed cost per dedicated Customer Success Manager	1	\$ 150,000	\$ 150,000	
SOW Item 4.0	Exchange Link	Annual SaaS State Platform Infrastructure	1	\$ 300,000	\$ 300,000	
	Exchange Link SaaS	Annual SaaS License for Each PSAP calculated by the total number of authroized call taking and dispatch positions	10	\$ 3,660	\$ 36,600	
	Exchange Link NRC	NRC for each ECC deployed	1	\$ 1,000		\$ 1,000
SOW Item 5.0	Lightning Mobile	Agency Annual Bundle Pricing licenses a maxium number of named users. Customers can move up in tiers as needed for expanding customer utilization.	100	\$ 180	\$ 18,000	
			1,000	\$ 126	\$ 126,000	
			5,000	\$ 99	\$ 495,000	
			10,000	\$ 90	\$ 900,000	
			20,000	\$ 81	\$ 1,620,000	
SOW Item 6.0	Smart 911	Annual SaaS License for Each PSAP calculated by the total number of authroized call taking and dispatch positions	1	\$ 700	\$ 700	
SOW Item 7.0	Video as a ServicePlatform SaaS	Cost per stream per year. Minimum 400 streams and up to 2,000 streams	400	\$ 720	\$ 288,000	
		Cost per stream per year. 2,001 – 4,000	2,001	\$ 684	\$ 1,368,684	
		Cost per stream per year. Over 4,000 streams	4,000	\$ 648	\$ 2,592,000	
	Video Sharing Platform NRC	NRC Initial Video Sharing Platform deployment	1	\$ 90,000		\$ 90,000
	Video Sharing Platform NRC	Each additional Video Source (server integration) NRC	1	\$ 30,000		\$ 30,000
SOW Item 8.0	Collaborative Response Graphics	Indoor Mapping of Educational Facilities price per school building	1	\$ 4,500		\$ 4,500
	Annual Maintenance of CRGs	Annual review, update of CRGs priced per school building	1		\$ 600	\$ -

Exhibit E: Contractor Attachments

The following documents are attached and incorporated into the Contract:

1. RapidDeploy Certificate of Insurance (COI)
2. Motorola Subscription Software Agreement
3. Skyline Software Licensing Agreement

RAPIINC-01

BKELLY



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

7/10/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Wall Street Insurance 216 Main Street Suite 215 Edwards, CO 81632	CONTACT NAME: PHONE (A/C, No, Ext): (970) 926-4900		FAX (A/C, No):
	E-MAIL ADDRESS: info@wallstreetinsurance.com		
	INSURER(S) AFFORDING COVERAGE		NAIC #
	INSURER A : Lloyd's Synd 2623 (Beazley Furlonge Ltd)		
	INSURER B : Travelers Cas & Sur Co of Amer		
	INSURER C :		
INSURED RapidDeploy Inc 310 Comal St Bldg A Suite 200, #205 Austin, TX 78702-4597	INSURER D :		31194
	INSURER E :		
	INSURER F :		

COVERAGES

CERTIFICATE NUMBER:

REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR ☒ Errors & Omissions GEN'L AGGREGATE LIMIT APPLIES PER: ☒ POLICY ☐ PRO-JECT ☐ LOC OTHER:	X		ESM0539792864	10/11/2023	10/11/2024	EACH OCCURRENCE \$ 500,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 250,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 5,000,000 GENERAL AGGREGATE \$ 5,000,000 PRODUCTS - COMP/OP AGG \$ 5,000,000 Prof Liab/Cyber \$ 5,000,000
A	AUTOMOBILE LIABILITY ☐ ANY AUTO OWNED AUTOS ONLY ☒ HIRED AUTOS ONLY ☐ SCHEDULED AUTOS ☒ NON-OWNED AUTOS ONLY			ESM0539792864	10/11/2023	10/11/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 5,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
	UMBRELLA LIAB ☐ OCCUR EXCESS LIAB ☐ CLAIMS-MADE DED ☐ RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) ☐ If yes, describe under DESCRIPTION OF OPERATIONS below		N/A				PER STATUTE ☐ OTH-ER ☐ E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	Errors & Omissions			ESM0539792864	10/11/2023	10/11/2024	Each Claim 5,000,000
B	Crime			106993858	10/11/2023	10/11/2024	1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 Excess D&O Policy #: MLXSHS292514-02 / Aggregate limit: \$2,000,000 Eff: 3/17/2024 to 3/17/2025

The State of Minnesota as additional insured with regard to General Liability as required by written contract.

CERTIFICATE HOLDER

CANCELLATION

The State of Minnesota Department of Administration, Materials Management Division 50 Sherburne Ave. Saint Paul, MN 55155	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE

Motorola (MSI) Subscription Software Agreement

This Subscription Software Agreement (the “**Subscription Software Agreement**”) is entered into between Motorola Solutions, Inc., with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 (“**Motorola**”) and the entity set forth in the signature block below (“**Customer**”). Motorola and Customer will each be referred to herein as a “**Party**” and collectively as the “**Parties**”. This Agreement (as defined below) is effective as of the date of the last signature (the “**Effective Date**”).

1. Agreement.

1.1. Scope; Agreement Documents. This Subscription Software Agreement governs Customer’s purchase of cloud-based software as a service products and other software which is licensed to Customer by Motorola on a subscription basis (“**Subscription Software**”) and related services, which may be recurring or one-time (“**Services**”) provided by Motorola. Subscription Software and Services are collectively referred to as the “**Software and Services**”. Additional terms and conditions applicable to specific Software and Services are set forth in one or more addenda attached to this Subscription Software Agreement (each an “**Addendum**”, and collectively the “**Addenda**”). In addition, the Parties may agree upon statements of work, schedules, technical specifications, and other ordering documents setting forth the Software and Services to be purchased by Customer and provided by Motorola and additional rights and obligations of the Parties (the “**Ordering Documents**”). To the extent required by applicable procurement law, a proposal submitted by Motorola in response to a competitive procurement process will be included within the meaning of the term Ordering Documents. This Subscription Software Agreement, the Addenda, and any Ordering Documents collectively form the Parties’ “**Agreement**”.

1.2. Order of Precedence. Each Addendum will control with respect to conflicting terms in this Subscription Software Agreement, but only as applicable to the Software and Services described in such Addendum. Each Ordering Document will control with respect to conflicting terms in this Subscription Software Agreement or any Addenda, but only as applicable to the Software and Services described on such Ordering Document.

2. Subscription Software.

2.1. Delivery. During the applicable Subscription Term (as defined below), Motorola will provide to Customer the Subscription Software set forth in an Ordering Document, in accordance with the terms of the Agreement. Motorola will provide Customer advance notice (which may be provided electronically) of any planned downtime. Delivery will occur upon Customer’s receipt of credentials required for access to the Subscription Software or upon Motorola otherwise providing access to the Subscription Software. If agreed upon in an Ordering Document, Motorola will also provide Services related to such Subscription Software.

2.2. Modifications. Motorola may modify the Subscription Software, any associated recurring Services and any related systems so long as their functionality (as described in the applicable Ordering Document) is not materially degraded. Documentation (as defined below) for the Subscription Software may be updated to reflect such modifications. For clarity, new features or enhancements that are added to any Subscription Software or Services may be subject to additional Fees.

2.3. User Credentials. If applicable, Motorola will provide Customer with administrative user credentials for the Subscription Software, and Customer will ensure such administrative user credentials are accessed and used only by Customer's employees with training on their proper use. Customer will protect, and will cause its Authorized Users to protect, the confidentiality and security of all user credentials, including any administrative user credentials, and maintain user credential validity, including by updating passwords. Customer will be liable for any use of the Subscription Software through such user credential (including through any administrative user credentials), including any changes made to the Subscription Software or issues or user impact arising therefrom. To the extent Motorola provides Services to Customer in order to help resolve issues resulting from changes made to the Subscription Software through user credentials, including through any administrative user credentials, or issues otherwise created by Authorized Users, such Services will be billed to Customer on a time and materials basis, and Customer will pay all invoices in accordance with the payment terms below.

2.4. Beta Services. If Motorola makes any beta version of a software application ("**Beta Service**") available to Customer, Customer may choose to use such Beta Service at its own discretion, provided, however, that Customer will use the Beta Service solely for purposes of Customer's evaluation of such Beta Service, and for no other purpose. Customer acknowledges and agrees that all Beta Services are offered "as-is" and without any representations or warranties or other commitments or protections from Motorola. Motorola will determine the duration of the evaluation period for any Beta Service, in its sole discretion, and Motorola may discontinue any Beta Service at any time. Customer acknowledges that Beta Services, by their nature, have not been fully tested and may contain defects or deficiencies.

2.5. Customer Obligations. Customer will ensure that information Customer provides to Motorola in connection with receipt of Software and Services are accurate and complete in all material respects. Customer will make timely decisions and obtain any required management approvals that are reasonably necessary for Motorola to provide the Software and Services and perform its other duties under this Agreement. Unless the applicable Ordering Document states otherwise, Motorola may rely upon and is not required to evaluate, confirm, reject, modify, or provide advice concerning any assumptions or Customer information, decisions, or approvals described in this Section. If any assumptions in the Ordering Documents or information provided by Customer prove to be incorrect, or if Customer fails to perform any of its obligations under this Agreement, Motorola's ability to perform its obligations may be impacted and changes to the Agreement, including the scope, Fees, and performance schedule may be required.

2.6. Documentation. Software and Services may be delivered with documentation for the equipment, software, or data that specifies technical and performance features, capabilities, users, or operation, including training manuals, and other deliverables, such as reports, specifications, designs, plans, drawings, analytics, or other information (collectively, "**Documentation**"). Documentation is and will be owned by Motorola, unless otherwise expressly agreed in an Addendum or Ordering Document that certain Documentation will be owned by Customer. Motorola hereby grants Customer a limited, royalty-free, worldwide, non-exclusive license to use the Documentation solely for its internal business purposes in connection with the Software and Services.

2.7. Authorized Users. Customer will ensure its employees and Authorized Users comply with the terms of this Agreement and will be liable for all acts and omissions of its employees and Authorized Users. Customer is responsible for the secure management of Authorized Users'

names, passwords and login credentials for access to Software and Services. “**Authorized Users**” are Customer’s employees, full-time contractors engaged for the purpose of supporting the Software and Services that are not competitors of Motorola, and the entities (if any) specified in an Ordering Document or otherwise approved by Motorola in writing (email from an authorized Motorola signatory accepted), which may include affiliates or other Customer agencies.

2.8. Support of Downloaded Clients. If Customer purchases any Subscription Software that requires a client installed locally on Customer-Provided Equipment, Customer will be responsible for downloading and installing the current version of such client, as it may be updated from time to time. Motorola will use reasonable efforts to continue supporting any version of a client for forty-five (45) days following its release, but Motorola may update the current version of its client at any time, including for bug fixes, product improvements, and feature updates, and Motorola makes no representations or warranties that any Subscription Software will support prior versions of a client.

2.9. Export Control. Customer, its employees, and any other Authorized Users will not access or use the Software and Services in any jurisdiction in which the provision of such Software and Services is prohibited under applicable laws or regulations (a “**Prohibited Jurisdiction**”), and Customer will not provide access to the Software and Services to any government, entity, or individual located in a Prohibited Jurisdiction. Customer represents and warrants that (a) it and its Authorized Users are not named on any U.S. government list of persons prohibited from receiving U.S. exports, or transacting with any U.S. person; (b) it and its Authorized Users are not a national of, or a company registered in, any Prohibited Jurisdiction; (c) Customer will not permit its Authorized Users to access or use the Subscription Software or Services in violation of any U.S. or other applicable export embargoes, prohibitions or restrictions; and (d) Customer and its Authorized Users will comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer, its employees, and the Authorized Users are located.

3. Term and Termination.

3.1. Subscription Terms. The duration of Customer’s subscription to the first Subscription Software and any associated recurring Services ordered under this Subscription Software Agreement (or the first Subscription Software or recurring Service, if multiple are ordered at once) will commence upon delivery of such Subscription Software (and recurring Services, if applicable) and will continue for a twelve (12) month period or such longer period identified in an Ordering Document (the “**Initial Subscription Period**”). Following the Initial Subscription Period, Customer’s subscription to the Subscription Software and any recurring Services will automatically renew for additional twelve (12) month periods (each, a “**Renewal Subscription Year**”), unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. (The Initial Subscription Period and each Renewal Subscription Year will each be referred to herein as a “**Subscription Term**”). Motorola may increase Fees prior to any Renewal Subscription Year. In such case, Motorola will notify Customer of such proposed increase no later than thirty (30) days prior to commencement of such Renewal Subscription Year. Unless otherwise specified in the applicable Ordering Document, if Customer orders any additional Subscription Software or recurring Services under this Subscription Software Agreement during an in-process Subscription Term, the subscription for each new Subscription Software or recurring Service will (a) commence upon delivery of such Subscription Software or Service, and continue until

the conclusion of Customer's then-current Subscription Term (a "**Partial Subscription Year**"), and (b) automatically renew for Renewal Subscription Years thereafter, unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current Subscription Term. Thus, unless otherwise specified in the applicable Ordering Document, the Subscription Terms for all Subscription Software and recurring Services hereunder will be synchronized.

3.2. Term. The term of this Subscription Software Agreement ("**Term**") will commence on the Effective Date and continue until the expiration or termination of all Subscription Terms under this Subscription Software Agreement, unless this Subscription Software Agreement is earlier terminated in accordance with the terms herein.

3.3. Termination.

3.3.1. For Default. Either Party may terminate the Agreement or the applicable Addendum or Ordering Document if the other Party breaches a material obligation under the Agreement and does not cure such breach within thirty (30) days after receipt of notice of the breach or fails to produce a cure plan within such period of time. Notwithstanding the foregoing, Motorola may terminate the Agreement (or any Addendum or Ordering Documents hereunder), or suspend delivery of Subscription Software or Services, immediately upon notice to Customer if (a) Customer breaches **Section 10.3 – Subscription Software License**, **Section 10.4 – End User Licenses**, or **Section 10.5 – Customer Restrictions** of this Subscription Software Agreement, or any other provision related to Subscription Software license scope or restrictions set forth in an Addendum or Ordering Document, or (b) it determines that Customer's use of the Subscription Software poses, or may pose, a security or other risk or adverse impact to any Subscription Software, Motorola, Motorola's systems, or any third party (including other Motorola customers). Customer acknowledges that Motorola made a considerable investment of resources in the development, marketing, and distribution of the Subscription Software and Documentation, and that Customer's breach of the Agreement will result in irreparable harm to Motorola for which monetary damages would be inadequate. If Customer breaches this Agreement, in addition to termination, Motorola will be entitled to all available remedies at law or in equity (including immediate injunctive relief).

3.3.2. Addenda; Ordering Documents. Each Addendum and Ordering Document may be separately terminable as set forth therein.

3.3.3. Wind Down of Subscription Software. Motorola may terminate any Ordering Document and Subscription Term, in whole or in part, in the event Motorola plans to cease offering the applicable Subscription Software or Service to customers.

3.4. Suspension of Services. Motorola may terminate or suspend any Software and Services under an Ordering Document if Motorola determines: (a) the related Subscription Software license has expired or has terminated for any reason; (b) the applicable Subscription Software is being used on a hardware platform, operating system, or version not approved by Motorola; (c) Customer fails to make any payments when due; or (d) Customer fails to comply with any of its other obligations or otherwise delays Motorola's ability to perform.

3.5. Effect of Termination or Expiration. Upon termination for any reason or expiration of this Subscription Software Agreement, an Addendum, or an Ordering Document, Customer and the Authorized Users will stop use of any Subscription Software and return or destroy (at

Motorola's option) all Motorola Confidential Information in their possession or control and, as applicable, provide proof of such destruction. If Customer has any outstanding payment obligations under this Agreement, Motorola may accelerate and declare all such obligations of Customer immediately due and payable by Customer. Notwithstanding the reason for termination or expiration, Customer must pay Motorola for Software and Services already delivered. Customer has a duty to mitigate any damages under this Agreement, including in the event of default by Motorola and Customer's termination of this Agreement.

4. Payment and Invoicing.

4.1. Fees. Unless otherwise provided in an Ordering Document, Customer will prepay an annual subscription fee for each Subscription Software and associated recurring Service, and pay any fees specified for other Services provided hereunder in accordance with the applicable Addendum or Ordering Document (the "**Fees**"), before the commencement of each Subscription Term. For any Partial Subscription Year, the applicable annual subscription Fee will be prorated based on the number of months in the Partial Subscription Year. The annual subscription Fee for Subscription Software and associated recurring Services may include certain one-time Fees, such as start-up fees, license fees, or other fees set forth in an Ordering Document. Motorola will have the right to suspend the Subscription Software and any recurring Services if Customer fails to make any payments when due. Fees may be changed by Motorola at any time, except that Motorola will not change the applicable Fees during a Subscription Term.

4.2. Taxes. The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, "**Taxes**"), all of which will be paid by Customer, except as exempt by law, unless otherwise specified in an Ordering Document. If Motorola is required to pay any Taxes, Customer will reimburse Motorola for such Taxes (including any interest and penalties) within thirty (30) days after Customer's receipt of an invoice therefore. Motorola will be solely responsible for reporting taxes on its income and net worth.

4.3. Invoicing; Payment. Customer will pay Fees upon the earlier of (a) thirty (30) days prior to the commencement of the applicable Subscription Term, and (b) within thirty (30) days of the applicable invoice date, or as otherwise specified in the applicable Addendum or Ordering Document. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. Motorola may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in an Ordering Document. Customer acknowledges and agrees that a purchase order or other notice to proceed is not required for payment for Software and Services.

4.4. License True-Up. Motorola will have the right to conduct an audit of total user licenses credentialed by Customer for any Subscription Software during a Subscription Term, and Customer will cooperate with such audit. If Motorola determines that Customer's usage of the Subscription Software during the applicable Subscription Term exceeded the total number of licenses purchased by Customer, Motorola may invoice Customer for the additional licenses used by Customer, pro-rated for each additional license from the date such license was activated, and Customer will pay such invoice in accordance with the payment terms in this **Section 4 – Payment and Invoicing**.

5. Customer-Provided Equipment; Non-Motorola Content.

5.1. Customer-Provided Equipment. Certain components, including equipment and software, not provided by Motorola may be required for use of the Software and Services (“**Customer-Provided Equipment**”). Customer will be responsible, at its sole cost and expense, for providing and maintaining the Customer-Provided Equipment in good working order. Customer represents and warrants that it has all rights in Customer-Provided Equipment to permit Motorola to access and use the applicable Customer-Provided Equipment to provide the Software and Services under this Agreement, and such access and use will not violate any laws or infringe any third-party rights (including intellectual property rights). Customer (and not Motorola) will be fully liable for Customer-Provided Equipment, and Customer will immediately notify Motorola of any Customer-Provided Equipment damage, loss, change, or theft that may impact Motorola’s ability to provide the Software and Services under this Agreement, and Customer acknowledges that any such events may cause a change in the Fees or performance schedule under the applicable Ordering Document.

5.2. Non-Motorola Content. In certain instances, Customer may be permitted to access, use, or integrate Customer or third-party software, equipment, services, content, and data that is not provided by Motorola (collectively, “**Non-Motorola Content**”) with or through the Software and Services. If Customer accesses, uses, or integrates any Non-Motorola Content with the Software and Services, Customer will first obtain all necessary rights and licenses to permit Customer’s and its Authorized Users’ use of the Non-Motorola Content in connection with the Software and Services. Customer will also obtain the necessary rights for Motorola to use such Non-Motorola Content in connection with providing the Software and Services, including the right for Motorola to access, store, and process such Non-Motorola Content (e.g., in connection with the Subscription Software), and to otherwise enable interoperation with the Software and Services. Customer represents and warrants that it will obtain the foregoing rights and licenses prior to accessing, using, or integrating the applicable Non-Motorola Content with the Software and Services, and that Customer and its Authorized Users will comply with any terms and conditions applicable to such Non-Motorola Content. If any Non-Motorola Content require access to Customer Data (as defined below), Customer hereby authorizes Motorola to allow the provider of such Non-Motorola Content to access Customer Data, in connection with the interoperation of such Non-Motorola Content with the Software and Services. Customer acknowledges and agrees that Motorola is not responsible for, and makes no representations or warranties with respect to, the Non-Motorola Content (including any disclosure, modification, or deletion of Customer Data resulting from use of Non-Motorola Content or failure to properly interoperate with the Software and Services). If Customer receives notice that any Non-Motorola Content must be removed, modified, or disabled within the Software and Services, Customer will promptly do so. Motorola will have the right to disable or remove Non-Motorola Content if Motorola believes a violation of law, third-party rights, or Motorola’s policies is likely to occur, or if such Non-Motorola Content poses or may pose a security or other risk or adverse impact to the Software and Services, Motorola, Motorola’s systems, or any third party (including other Motorola customers). Motorola may provide certain Non-Motorola Content as an authorized sales representative of a third party as set out in an Ordering Document. As an authorized sales representative, the third party’s terms and conditions, as set forth in the Ordering Document, will apply to any such sales. Any orders for such Non-Motorola Content will be filled by the third party. Nothing in this Section will limit the exclusions set forth in **Section 7.1 – Intellectual Property Infringement**.

5.3. End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Content software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Software. Customer will comply, and ensure its Authorized Users

comply, with any such additional terms applicable to third-party equipment or software. If provided for in the separate third party license, Customer may have a right to receive source code for such software; a copy of such source code may be obtained free of charge by contacting Motorola.

6. Representations and Warranties.

6.1. Mutual Representations and Warranties. Each Party represents and warrants to the other Party that (a) it has the right to enter into the Agreement and perform its obligations hereunder, and (b) the Agreement will be binding on such Party.

6.2. WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS AGREEMENT, SOFTWARE AND SERVICES PURCHASED HEREUNDER ARE PROVIDED “AS IS” AND WITH ALL FAULTS. WARRANTIES SET FORTH IN THE AGREEMENT ARE THE COMPLETE WARRANTIES FOR THE SOFTWARE AND SERVICES AND MOTOROLA DISCLAIMS ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND QUALITY. MOTOROLA DOES NOT REPRESENT OR WARRANT THAT USE OF THE SOFTWARE AND SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF SECURITY VULNERABILITIES, OR THAT THEY WILL MEET CUSTOMER’S PARTICULAR REQUIREMENTS.

7. Indemnification.

7.1. Intellectual Property Infringement. Motorola will defend Customer against any third-party claim alleging that a Motorola-developed Subscription Software (the “**Infringing Product**”) directly infringes a United States patent or copyright (“**Infringement Claim**”), and Motorola will pay all damages finally awarded against Customer by a court of competent jurisdiction for an Infringement Claim, or agreed to in writing by Motorola in settlement of an Infringement Claim. Motorola’s duties under this **Section 7.1 – Intellectual Property Infringement** are conditioned upon: (a) Customer promptly notifying Motorola in writing of the Infringement Claim; (b) Motorola having sole control of the defense of the suit and all negotiations for its settlement or compromise; and (c) Customer cooperating with Motorola and, if requested by Motorola, providing reasonable assistance in the defense of the Infringement Claim.

7.1.1. If an Infringement Claim occurs, or in Motorola’s opinion is likely to occur, Motorola may at its option and expense: (a) procure for Customer the right to continue using the Infringing Product; (b) replace or modify the Infringing Product so that it becomes non-infringing; or (c) grant Customer a pro-rated refund of any amounts pre-paid for the Infringing Product.

7.1.2. In addition to the other damages disclaimed under this Agreement, Motorola will have no duty to defend or indemnify Customer for any Infringement Claim that arises from or is based upon: (a) Customer Data, Customer-Provided Equipment, Non-Motorola Content, or third-party equipment, hardware, software, data, or other third-party materials; (b) the combination of the Subscription Software or Services with any products or materials not provided by Motorola; (c) any Subscription Software or Service designed, modified, or manufactured in accordance with Customer’s designs, specifications, guidelines or instructions; (d) a modification of the Subscription Software or Services by a party other than Motorola; (e) use of the Subscription Software or Services in a manner for which the Subscription Software or Service was not designed or that is inconsistent with the terms of this Agreement; or (f) the failure by Customer

to use or install an update to the Subscription Software or Services that is intended to correct the claimed infringement. In no event will Motorola's liability resulting from an Infringement Claim extend in any way to any payments due on a royalty basis, other than a reasonable royalty based upon revenue derived by Motorola from Customer from sales or license of the Infringing Product.

7.1.3. This **Section 7.1 – Intellectual Property Infringement** provides Customer's sole and exclusive remedies and Motorola's entire liability in the event of an Infringement Claim. For clarity, the rights and remedies provided in this Section are subject to, and limited by, the restrictions set forth in **Section 8 – Limitation of Liability** below.

7.2. Customer Indemnity. Customer will defend, indemnify, and hold Motorola and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to (a) Customer-Provided Equipment, Customer Data, or Non-Motorola Content, including any claim, demand, action, or proceeding alleging that any such equipment, data, or materials (or the integration or use thereof with the Software and Services) infringes or misappropriates a third-party intellectual property or other right, violates applicable law, or breaches the Agreement, (b) Customer-Provided Equipment's failure to meet the minimum requirements set forth in the applicable Documentation or match the applicable specifications provided to Motorola by Customer in connection with the Subscription Software or Services; (c) Customer's (or its service providers, agents, employees, or Authorized User's) negligence or willful misconduct; and (d) Customer's or its Authorized User's breach of this Agreement. This indemnity will not apply to the extent any such claim is caused by Motorola's use of Customer-Provided Equipment, Customer Data, or Non-Motorola Content in violation of the Agreement. Motorola will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Motorola will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

8. Limitation of Liability.

8.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, MOTOROLA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "**MOTOROLA PARTIES**") WILL NOT BE LIABLE IN CONNECTION WITH THIS AGREEMENT (WHETHER UNDER MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR, ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

8.2. DIRECT DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF THE MOTOROLA PARTIES, WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THE AGREEMENT WILL NOT EXCEED THE TOTAL FEES PAID FOR THE SUBSCRIPTION SOFTWARE TO WHICH THE CLAIM IS RELATED DURING THE CONSECUTIVE TWELVE

(12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FROM WHICH THE FIRST CLAIM AROSE.

8.3. ADDITIONAL EXCLUSIONS. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, MOTOROLA WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) CUSTOMER DATA, INCLUDING ITS TRANSMISSION TO MOTOROLA, OR ANY OTHER DATA AVAILABLE THROUGH THE SUBSCRIPTION SOFTWARE OR SERVICES; (B) CUSTOMER-PROVIDED EQUIPMENT, NON-MOTOROLA CONTENT, CUSTOMER'S SITES, OR THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, DATA, OR OTHER THIRD-PARTY MATERIALS, OR THE COMBINATION OF THE SUBSCRIPTION SOFTWARE OR SERVICES WITH ANY OF THE FOREGOING; (C) LOSS OF DATA OR HACKING, RANSOMWARE, OR OTHER THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF SUBSCRIPTION SOFTWARE OR SERVICES BY ANY PERSON OTHER THAN MOTOROLA; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH OR BY THE SUBSCRIPTION SOFTWARE AND SERVICES; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; (G) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (H) DISRUPTION OF OR DAMAGE TO CUSTOMER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (I) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE SUBSCRIPTION SOFTWARE OR SERVICES, OR INTERPRETATION, USE, OR MISUSE THEREOF; (J) TRACKING AND LOCATION-BASED SERVICES; (K) BETA SERVICES; OR (L) CUSTOMER'S OR ANY AUTHORIZED USER'S BREACH OF THIS AGREEMENT OR MISUSE OF THE SUBSCRIPTION SOFTWARE OR SERVICES.

8.4. Voluntary Remedies. Motorola is not obligated to remedy, repair, replace, or refund the purchase price for the disclaimed issues in **Section 8.3 – Additional Exclusions** above, but if Motorola agrees to provide Services to help resolve such issues, Customer will reimburse Motorola for its reasonable time and expenses, including by paying Motorola any Fees set forth in an Ordering Document for such Services, if applicable.

8.5. Statute of Limitations. Customer may not bring any claims against a Motorola Party in connection with this Agreement or the Software and Services more than one (1) year after the date of accrual of the cause of action.

9. Confidentiality.

9.1. Confidential Information. “**Confidential Information**” means any and all non-public information provided by one Party (“**Discloser**”) to the other (“**Recipient**”) that is disclosed under this Agreement in oral, written, graphic, machine recognizable, or sample form, being clearly designated, labeled or marked as confidential or its equivalent or that a reasonable businessperson would consider non-public and confidential by its nature. With respect to Motorola, Confidential Information will also include Software and Services, and Documentation, as well as any other information relating to the Software and Services. The nature and existence of this Agreement are considered Confidential Information of the Parties. In order to be considered Confidential Information, information that is disclosed orally must be identified as confidential at the time of disclosure and confirmed by Discloser by submitting a written document to Recipient within thirty (30) days after such disclosure. The written document must

contain a summary of the Confidential Information disclosed with enough specificity for identification purpose and must be labeled or marked as confidential or its equivalent.

9.2. Obligations of Confidentiality. During the Term and for a period of three (3) years from the expiration or termination of this Agreement, Recipient will (a) not disclose Confidential Information to any third party, except as expressly permitted in this **Section 9 – Confidentiality**; (b) restrict disclosure of Confidential Information to only those employees (including, employees of any wholly owned subsidiary, a parent company, any other wholly owned subsidiaries of the same parent company), agents or consultants who must access the Confidential Information for the purpose of, and who are bound by confidentiality terms substantially similar to those in, this Agreement; (c) not copy, reproduce, reverse engineer, de-compile or disassemble any Confidential Information; (d) use the same degree of care as for its own information of like importance, but at least use reasonable care, in safeguarding against disclosure of Confidential Information; (e) promptly notify Discloser upon discovery of any unauthorized use or disclosure of the Confidential Information and take reasonable steps to regain possession of the Confidential Information and prevent further unauthorized actions or other breach of this Agreement; and (f) only use the Confidential Information as needed to fulfill its obligations and secure its rights under this Agreement.

9.3. Exceptions. Recipient is not obligated to maintain as confidential any information that Recipient can demonstrate by documentation (a) is publicly available at the time of disclosure or becomes available to the public without breach of this Agreement; (b) is lawfully obtained from a third party without a duty of confidentiality to Discloser; (c) is otherwise lawfully known to Recipient prior to such disclosure without a duty of confidentiality to Discloser; or (d) is independently developed by Recipient without the use of, or reference to, any of Discloser's Confidential Information or any breach of this Agreement. Additionally, Recipient may disclose Confidential Information to the extent required by law, including a judicial or legislative order or proceeding.

9.4. Ownership of Confidential Information. All Confidential Information is and will remain the property of Discloser and will not be copied or reproduced without the express written permission of Discloser (including as permitted herein). Within ten (10) days of receipt of Discloser's written request, Recipient will return or destroy all Confidential Information to Discloser along with all copies and portions thereof, or certify in writing that all such Confidential Information has been destroyed. However, Recipient may retain (a) one (1) archival copy of the Confidential Information for use only in case of a dispute concerning this Agreement and (b) Confidential Information that has been automatically stored in accordance with Recipient's standard backup or recordkeeping procedures, provided, however that Recipient will remain subject to the obligations of this Agreement with respect to any Confidential Information retained subject to clauses (a) or (b). No license, express or implied, in the Confidential Information is granted to the Recipient other than to use the Confidential Information in the manner and to the extent authorized by this Agreement. Discloser represents and warrants that it is authorized to disclose any Confidential Information it discloses pursuant to this Agreement.

10. Proprietary Rights and Subscription Software License; Data; Feedback.

10.1. Data Definitions. The following terms will have the stated meanings: “**Customer Contact Data**” means data Motorola collects from Customer, its Authorized Users, and their end users for business contact purposes, including marketing, advertising, licensing and sales purposes;

“**Service Use Data**” means data generated by Customer’s use of the Software and Services or by Motorola’s support of the Software and Services, including personal information, product performance and error information, activity logs and date and time of use; “**Customer Data**” means data, information, and content, including images, text, videos, documents, audio, telemetry, location and structured data base records, provided by, through, or on behalf of Customer, its Authorized Users, and their end users through the use of the Software and Services. Customer Data does not include Customer Contact Data, Service Use Data, or information from publicly available sources or other Third-Party Data or Motorola Data; “**Third-Party Data**” means information obtained by Motorola from publicly available sources or its third party content providers and made available to Customer through the Subscription Software or Services; “**Motorola Data**” means data owned or licensed by Motorola; “**Feedback**” means comments or information, in oral or written form, given to Motorola by Customer or Authorized Users, including their end users, in connection with or relating to the Subscription Software or Services; and “**Process**” or “**Processing**” means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

10.2. Motorola Materials. Customer acknowledges that Motorola may use or provide Customer with access to software, tools, data, and other materials, including designs, utilities, models, methodologies, systems, and specifications, which Motorola has developed or licensed from third parties (including any corrections, bug fixes, enhancements, updates, modifications, adaptations, translations, de-compilations, disassemblies, or derivative works of the foregoing, whether made by Motorola or another party) (collectively, “**Motorola Materials**”). The Software and Services, Motorola Data, Third-Party Data, and Documentation, are considered Motorola Materials. Except when Motorola has expressly transferred title or other interest to Customer by way of an Addendum or Ordering Document, the Motorola Materials are the property of Motorola or its licensors, and Motorola or its licensors retain all right, title and interest in and to the Motorola Materials (including, all rights in patents, copyrights, trademarks, trade names, trade secrets, know-how, other intellectual property and proprietary rights, and all associated goodwill and moral rights). For clarity, this Agreement does not grant to Customer any shared development rights in or to any Motorola Materials or other intellectual property, and Customer agrees to execute any documents and take any other actions reasonably requested by Motorola to effectuate the foregoing. Motorola and its licensors reserve all rights not expressly granted to Customer, and no rights, other than those expressly granted herein, are granted to Customer by implication, estoppel or otherwise. Customer will not modify, disassemble, reverse engineer, derive source code or create derivative works from, merge with other software, distribute, sublicense, sell, or export the Software and Services or other Motorola Materials, or permit any third party to do so.

10.3. Subscription Software License. Subject to Customer’s and its Authorized Users’ compliance with the Agreement (including payment terms), Motorola hereby grants Customer and its Authorized Users a limited, non-transferable, non-sublicenseable, and non-exclusive license to use the Subscription Software identified in an Ordering Document, and the associated Documentation, solely for Customer’s internal business purposes. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in an Ordering Document (if applicable), and will continue for the applicable Subscription Term. Customer may access, and use the Subscription Software only in Customer’s owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized

Users using authorized mobile or handheld devices may also log into and access the Subscription Software remotely from any location. No custom development work will be performed under this Agreement.

10.4. End User Licenses. Notwithstanding any provision to the contrary in the Agreement, certain Non-Motorola Content software are governed by a separate license, EULA, or other agreement, including terms governing third-party equipment or software, such as open source software, included in the Subscription Software. Customer will comply, and ensure its Authorized Users comply, with any such additional terms applicable to third-party equipment or software. If provided for in the separate third party license, Customer may have a right to receive source code for such software; a copy of such source code may be obtained free of charge by contacting Motorola.

10.5. Customer Restrictions. Customers and Authorized Users will comply with the applicable Documentation and the copyright laws of the United States and all other relevant jurisdictions (including the copyright laws where Customer uses the Subscription Software) in connection with their use of the Subscription Software. Customer will not, and will not allow others, including the Authorized Users, to make the Subscription Software available for use by unauthorized third parties, including via a commercial rental or sharing arrangement; reverse engineer, disassemble, or reprogram software used to provide the Subscription Software or any portion thereof to a human-readable form; modify, create derivative works of, or merge the Subscription Software or software used to provide the Subscription Software with other software; copy, reproduce, distribute, lend, or lease the Subscription Software, software used to provide the Subscription Software, or Documentation for or to any third party; take any action that would cause the Subscription Software or Documentation to be placed in the public domain; use the Subscription Software to compete with Motorola; remove, alter, or obscure, any copyright or other notice; share user credentials (including among Authorized Users); use the Subscription Software to store or transmit malicious code; or attempt to gain unauthorized access to the Subscription Software or its related systems or networks.

10.6. Ownership of Customer Data. Customer retains all right, title and interest, including intellectual property rights, if any, in and to Customer Data. Motorola acquires no rights to Customer Data except those rights granted under this Agreement including the right to Process and use the Customer Data as set forth in **Section 10.7 – Processing Customer Data** below and in other applicable Addenda. The Parties agree that with regard to the Processing of personal information which may be part of Customer Data, Customer is the controller and Motorola is the processor, and may engage sub-processors pursuant to **Section 10.7.3 – Sub-processors**.

10.7. Processing Customer Data.

10.7.1. Motorola Use of Customer Data. To the extent permitted by law, Customer grants Motorola and its subcontractors a right to use Customer Data and a royalty-free, worldwide, non-exclusive license to use Customer Data (including to process, host, cache, store, reproduce, copy, modify, combine, analyze, create derivative works from such Customer Data and to communicate, transmit, and distribute such Customer Data to third parties engaged by Motorola) to (a) perform Services and provide the Subscription Software under the Agreement, (b) analyze the Customer Data to operate, maintain, manage, and improve Motorola products and services, and (c) create new products and services. Customer agrees that this Agreement, along with the Documentation, are Customer's complete and final documented instructions to

Motorola for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the Change Order process. Customer represents and warrants to Motorola that Customer's instructions, including appointment of Motorola as a processor or sub-processor, have been authorized by the relevant controller.

10.7.2. Collection, Creation, Use of Customer Data. Customer further represents and warrants that the Customer Data, Customer's collection, creation, and use of the Customer Data (including in connection with Motorola's Software and Services), and Motorola's use of such Customer Data in accordance with the Agreement, will comply with all laws and will not violate any applicable privacy notices or infringe any third-party rights (including intellectual property and privacy rights). It is Customer's responsibility to obtain all required consents, provided all necessary notices, and met any other applicable legal requirements with respect to collection and use (including Motorola's use) of the Customer Data as described in the Agreement.

10.7.3. Sub-processors. Customer agrees that Motorola may engage sub-processors who in turn may engage additional sub-processors to Process personal data in accordance with this Agreement. When engaging sub-processors, Motorola will enter into agreements with the sub-processors to bind them to data processing obligations to the extent required by law.

10.8. Data Retention and Deletion. Except as expressly provided otherwise under the Agreement, Motorola will delete all Customer Data following termination or expiration of this Subscription Software Agreement or the applicable Addendum or Ordering Document, with such deletion to occur no later than ninety (90) days following the applicable date of termination or expiration, unless otherwise required to comply with applicable law. Any requests for the exportation or download of Customer Data must be made by Customer to Motorola in writing before expiration or termination, subject to **Section 14.9 – Notices**. Motorola will have no obligation to retain such Customer Data beyond expiration or termination unless the Customer has purchased extended storage from Motorola through a mutually executed Ordering Document.

10.9. Service Use Data. Customer understands and agrees that Motorola may collect and use Service Use Data for its own purposes, including the uses described below. Motorola may use Service Use Data to (a) operate, maintain, manage, and improve existing and create new products and services, (b) test products and services, (c) to aggregate Service Use Data and combine it with that of other users, and (d) to use anonymized or aggregated data for marketing, research or other business purposes. Service Use Data may be disclosed to third parties. It is Customer's responsibility to notify Authorized Users of Motorola's collection and use of Service Use Data and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use, and Customer represents and warrants to Motorola that it has complied and will continue to comply with this Section.

10.10. Third-Party Data and Motorola Data. Motorola Data and Third-Party Data may be available to Customer through the Software and Services. Customer and its Authorized Users may use Motorola Data and Third-Party Data as permitted by Motorola and the applicable Third-Party Data provider, as described in the applicable Addendum. Unless expressly permitted in the applicable Addendum, Customer will not, and will ensure its Authorized Users will not: (a) use the Motorola Data or Third-Party Data for any purpose other than Customer's internal business purposes; (b) disclose the data to third parties; (c) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or

commercially exploit the data in any manner; (d) use such data in violation of applicable laws; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third-Party Data will immediately terminate upon termination or expiration of the applicable Addendum, Ordering Document, or this Subscription Software Agreement. Further, Motorola or the applicable Third-Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third-Party Data if Motorola or such Third-Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or Motorola's agreement with the applicable Third-Party Data provider. Upon termination of Customer's rights to use any Motorola Data or Third-Party Data, Customer and all Authorized Users will immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola will have no liability for Third-Party Data or Motorola Data available through the Software and Services. Motorola and its Third-Party Data providers reserve all rights in and to Motorola Data and Third-Party Data not expressly granted in an Addendum or Ordering Document.

10.11. Feedback. Any Feedback provided by Customer is entirely voluntary, and will not create any confidentiality obligation for Motorola, even if designated as confidential by Customer. Motorola may use, reproduce, license, and otherwise distribute and exploit the Feedback without any obligation or payment to Customer or Authorized Users and Customer represents and warrants that it has obtained all necessary rights and consents to grant Motorola the foregoing rights.

10.12. Improvements; Software and Services. The Parties agree that, notwithstanding any provision of this Subscription Software Agreement or the Agreement to the contrary, all fixes, modifications and improvements to the services or products conceived of or made by or on behalf of Motorola that are based either in whole or in part on the Feedback, Customer Data, or Service Use Data (or otherwise) are the exclusive property of Motorola and all right, title and interest in and to such fixes, modifications or improvements will vest solely in Motorola. Customer agrees to execute any written documents necessary to assign any intellectual property or other rights it may have in such fixes, modifications or improvements to Motorola.

11. Motorola as a Controller or Joint Controller. In all instances where Motorola acts as a controller of data, it will comply with the applicable provisions of the Motorola Privacy Statement at https://www.motorolasolutions.com/en_us/about/privacy-policy.html#privacystatement, as may be updated from time to time. Motorola holds all Customer Contact Data as a controller and shall Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In instances where Motorola is acting as a joint controller with Customer, the Parties will enter into a separate Addendum to the Agreement to allocate the respective roles as joint controllers.

12. Force Majeure; Delays Caused by Customer.

12.1. Force Majeure. Except for Customer's payment obligations hereunder, neither Party will be responsible for nonperformance or delayed performance due to events outside of its reasonable control. If performance will be significantly delayed, the affected Party will provide

notice to the other Party, and the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule.

12.2. Delays Caused by Customer. Motorola's performance of the Software and Services will be excused for delays caused by Customer or its Authorized Users or subcontractors, or by failure of any assumptions set forth in this Agreement (including in any Addendum or Ordering Document). In the event of a delay under this **Section 12.2 – Delays Caused by Customer**, (a) Customer will continue to pay the Fees as required hereunder, (b) the Parties will agree (in writing) upon a reasonable extension to any applicable performance schedule, and (c) Customer will compensate Motorola for its out-of-pocket costs incurred due to the delay (including those incurred by Motorola's affiliates, vendors, and subcontractors).

13. Disputes. The Parties will use the following procedure to resolve any disputes relating to or arising out of this Agreement (each, a "**Dispute**"):

13.1. Governing Law. All matters relating to or arising out of the Agreement are governed by the laws of the State of Illinois, unless Customer is the United States Government (or an agency thereof), in which case all matters relating to or arising out of the Agreement will be governed by the laws of the State in which the Software and Services are provided. The terms of the U.N. Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act will not apply.

13.2. Negotiation; Mediation. Either Party may initiate dispute resolution procedures by sending a notice of Dispute ("**Notice of Dispute**") to the other Party. The Parties will attempt to resolve the Dispute promptly through good faith negotiations, including timely escalation of the Dispute to executives who have authority to settle the Dispute (and who are at a higher level of management than the persons with direct responsibility for the matter). If a Dispute is not resolved through negotiation, either Party may initiate mediation by sending a notice of mediation ("**Notice of Mediation**") to the other Party. The Parties will choose an independent mediator within thirty (30) days of such Notice of Mediation. Neither Party may unreasonably withhold consent to the selection of a mediator, but if the Parties are unable to agree upon a mediator, either Party may request that the American Arbitration Association nominate a mediator. Each Party will bear its own costs of mediation, but the Parties will share the cost of the mediator equally. Each Party will participate in the mediation in good faith and will be represented at the mediation by a business executive with authority to settle the Dispute. All in person meetings under this **Section 13.2 – Negotiation; Mediation** will take place in Chicago, Illinois, and all communication relating to the Dispute resolution will be maintained in strict confidence by the Parties. Notwithstanding the foregoing, any Dispute arising from or relating to Motorola's intellectual property rights will not be subject to negotiation or mediation in accordance with this Section, but instead will be decided by a court of competent jurisdiction, in accordance with **Section 13.3 – Litigation, Venue, Jurisdiction** below.

13.3. Litigation, Venue, Jurisdiction. If the Dispute has not been resolved by mediation within sixty (60) days from the Notice of Mediation, either Party may submit the Dispute exclusively to a court in Cook County, Illinois. Each Party expressly consents to the exclusive jurisdiction of such courts for resolution of any Dispute and to enforce the outcome of any mediation.

14. General.

14.1. Compliance with Laws. Each Party will comply with applicable laws in connection with the performance of its obligations under this Agreement, including that Customer will ensure its and its Authorized Users' use of the Software and Services complies with law (including privacy laws), and Customer will obtain any FCC and other licenses or authorizations (including licenses or authorizations required by foreign regulatory bodies) required for its and its Authorized Users' use of the Software and Services. Motorola may, at its discretion, cease providing or otherwise modify Software and Services (or any terms related thereto in an Addendum or Ordering Document), in order to comply with any changes in applicable law.

14.2. Audit; Monitoring. Motorola will have the right to monitor and audit use of the Subscription Software, which may also include access by Motorola to Customer Data and Service Use Data. Customer will provide notice of such monitoring to its Authorized Users and obtain any required consents, including individual end users, and will cooperate with Motorola in any monitoring or audit. Customer will maintain during the Term, and for two (2) years thereafter, accurate records relating to the Subscription Software licenses granted under this Agreement to verify compliance with this Agreement. Motorola or a third party ("**Auditor**") may inspect Customer's and, as applicable, Authorized Users' premises, books, and records. Motorola will pay expenses and costs of the Auditor, unless Customer is found to be in violation of the terms of the Agreement, in which case Customer will be responsible for such expenses and costs.

14.3. Assignment and Subcontracting. Neither Party may assign or otherwise transfer this Agreement without the prior written approval of the other Party. Motorola may assign or otherwise transfer this Agreement or any of its rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of its assets, (c) as part of a corporate reorganization, or (d) to a subsidiary corporation. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns.

14.4. Waiver. A delay or omission by either Party to exercise any right under this Agreement will not be construed to be a waiver of such right. A waiver by either Party of any of the obligations to be performed by the other, or any breach thereof, will not be construed to be a waiver of any succeeding breach or of any other obligation. All waivers must be in writing and signed by the Party waiving its rights.

14.5. Severability. If any provision of the Agreement is found by a court of competent jurisdiction to be invalid, illegal, or otherwise unenforceable, such provision will be deemed to be modified to reflect as nearly as possible the original intentions of the Parties in accordance with applicable law. The remaining provisions of this Agreement will not be affected, and each such provision will be valid and enforceable to the full extent permitted by applicable law.

14.6. Independent Contractors. Each Party will perform its duties under this Agreement as an independent contractor. The Parties and their personnel will not be considered to be employees or agents of the other Party. Nothing in this Agreement will be interpreted as granting either Party the right or authority to make commitments of any kind for the other. This Agreement will not constitute, create, or be interpreted as a joint venture, partnership, or formal business organization of any kind.

14.7. Third-Party Beneficiaries. The Agreement is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Agreement will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties. Notwithstanding

the foregoing, a licensor or supplier of third-party software included in the Subscription Software will be a direct and intended third-party beneficiary of this Agreement.

14.8. Interpretation. The section headings in this Agreement are included only for convenience. The words “including” and “include” will be deemed to be followed by the phrase “without limitation”. This Agreement will be fairly interpreted in accordance with its terms and conditions and not for or against either Party.

14.9. Notices. Notices required under this Agreement to be given by one Party to the other must be in writing and either personally delivered or sent to the address provided by the other Party by certified mail, return receipt requested and postage prepaid (or by a recognized courier service, such as FedEx, UPS, or DHL), and will be effective upon receipt.

14.10. Cumulative Remedies. Except as specifically stated in this Agreement, all remedies provided for in this Agreement will be cumulative and in addition to, and not in lieu of, any other remedies available to either Party at law, in equity, by contract, or otherwise. Except as specifically stated in this Agreement, the election by a Party of any remedy provided for in this Agreement or otherwise available to such Party will not preclude such Party from pursuing any other remedies available to such Party at law, in equity, by contract, or otherwise.

14.11. Survival. The following provisions will survive the expiration or termination of this Agreement for any reason: **Section 2.5 – Customer Obligations; Section 3 – Term and Termination; Section 4 – Payment and Invoicing; Section 6.2 – Warranty Disclaimer; Section 7.2 – Customer Indemnity; Section 8 – Limitation of Liability; Section 9 – Confidentiality; Section 10 – Proprietary Rights and Subscription Software License; Data; Feedback; Section 12 – Force Majeure; Delays Caused by Customer; Section 13 – Disputes; and Section 14 – General.**

Entire Agreement. This Agreement, including all Addenda and Ordering Documents, constitutes the entire agreement of the Parties regarding the subject matter hereto, and supersedes all previous agreements, proposals, and understandings, whether written or oral, relating to this subject matter. This Agreement may be executed in multiple counterparts, and will have the same legal force and effect as if the Parties had executed it as a single document. The Parties may sign in writing or by electronic signature. An electronic signature, facsimile copy, or computer image of a signature, will be treated, and will have the same effect as an original signature, and will have the same effect, as an original signed copy of this document. This Agreement may be amended or modified only by a written instrument signed by authorized representatives of both Parties. The preprinted terms and conditions found on any Customer purchase order, acknowledgment, or other form will not be considered an amendment or modification or part of this Agreement, even if a representative of each Party signs such document.

Skyline Software Licensing Agreement

This Software License Agreement, ("Agreement") is between Skyline Technology Solutions, LLC ("Skyline") and the customer (individual or entity) that has downloaded or otherwise procured the licensed Software Product (as defined below) for use as an end user ("User"). User agrees to abide by the terms of this Agreement.

1. Definitions.

- a. "Software Product" means the proprietary Skyline software product(s) provided to User in connection with this Agreement. It includes the live video streaming, sharing, transcoding and/or management software application, and those appliances, programs, models, rules, Documentation and all modifications made thereto by Skyline. "Software Product" also includes any third-party embedded software products licensed by Skyline that are provided as part of the video streaming, sharing, transcoding and/or management software application. Unless otherwise noted, the Software Product and Documentation are referred to collectively herein as "Software Product."
- b. "Derivative Works" means any modifications, changes or enhancements to the Software Product made by the User, or on behalf of the user by Skyline or a third party.
- c. "Acceptance" means that the User has accepted the terms of this Agreement and has Accepted this agreement by signature of its authorized official.
- d. "Date of this Agreement" means the Effective Date.
- e. "Documentation" means any supporting product help and technical specifications documentation provided by Skyline with the Software Product to User.
- f. "Effective Date" means the date User first ordered the Software Product or the initial delivery date of the Software Product (whichever is earlier).
- g. "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the functionality of the Software Product.
- h. "Administrative Users" means individual users with rights to perform application administrative functions.
- i. "Permitted End Users" means any employee of the User and there shall be no limit on the number of such qualified Permitted End Users who may use the Software Product.
- j. "License Fee" means the fee due to Skyline as set forth in any ordering document or otherwise identified by Skyline in a proposal or invoice.

2. User's Duties.

- a. Ownership of Intellectual Property. Except for certain third-party software, which is the intellectual property of the applicable third-party licensors, the Software Product is Skyline's intellectual property. Skyline shall retain sole and exclusive ownership of all right, title, and interest in and to the Software Product, including Documentation and associated deliverables, all copies thereof, and all modifications and enhancements thereto made by Skyline at Skyline's

initiative (including ownership of all copyrights, trademarks, trade secrets and other intellectual property rights pertaining thereto), subject only to the right and license expressly granted to User herein. This Agreement does not provide User with title or ownership of the Software Product but only a license as described more fully herein.

- b. Enhancements or modifications created by Skyline prior to this Agreement or outside of this Agreement and used by Skyline to fulfill its obligations under this Agreement will remain the property of Skyline.
- c. Ownership of software, enhancements, modifications and derivative works thereof (including any changes which incorporate any of Users ideas, feedback or suggestions), intellectual property and deliverables developed for User by Skyline shall be owned and retained solely by Skyline.
- d. Confidentiality Agreement. User agrees to abide by the terms of Paragraph 4.
- e. Report to Skyline. User agrees to abide by the terms of Paragraph 5.
- f. Compliance with Laws. User will comply with all applicable laws and regulations in effect during the term of the Agreement as they apply to User's rights and obligations under the Agreement.

3. License.

UPON FULL EXECUTION OF THIS AGREEMENT, SUBJECT TO USER'S PAYMENT OF THE REQUIRED LICENSE FEES TO SKYLINE, SKYLINE GRANTS TO USER A NON-EXCLUSIVE, PERPETUAL, NON-ASSIGNABLE, NON-TRANSFERABLE LICENSE TO USE THE SOFTWARE PRODUCT AS PROVIDED IN THIS AGREEMENT. THE SOFTWARE PRODUCT IS LICENSED BY SKYLINE TO USER ACCORDING TO THE TERMS OF THIS AGREEMENT. ALL RIGHTS NOT EXPRESSLY GRANTED TO USER HEREIN ARE RESERVED TO SKYLINE OR ITS LICENSORS.

- a. Use of Software Product. The Software Product may only be installed by Skyline on hardware that is pre-approved by Skyline. User may not make any copies of the Software Product.
- b. Modifications to Software Product. User may not modify, enhance or customize the Software Product.
- c. Transfer to Third Parties. User may not transfer this Software Product or assign this Agreement in whole or in part, to third parties without prior notification to Skyline.
- d. Incorporation of Third-Party Software. Software Product may contain or be derived from materials of third-party licensors. The restrictions and obligations applicable to User's use of the Software Product under this Agreement extend to any such third-party licensor materials. Pursuant to its agreements with these third parties, Skyline grants to User a non-exclusive, non-transferable license to use any such third-party software solely in conjunction with the Software Product.

- e. Restrictions. User may not lease, use, copy, rent, modify, distribute or sublicense the Software Product except as otherwise set forth herein. User may not reverse engineer, decompile, disassemble, or otherwise translate the Software Product.
 - f. Permitted End Users. There are no limits to the number of End Users permitted to access the Software Product.
 - g. Default. Skyline may terminate this Agreement upon the User's breach of a material term following reasonable written notice of the breach to User and a 10-day cure period. Skyline will have no obligation to refund the Annual Fee In the event of a termination of this Agreement by Skyline caused by a breach by User. In the event of such termination, the User will be required to discontinue its use of the Software Product.
 - h. Term. The license granted to the User hereunder shall commence on the Effective Date and shall continue in perpetuity, unless and until terminated as provided in this Section. The obligations set forth in Sections 2, 4, 7, 8, 9 and this Section shall survive termination or expiration of this Agreement.
 - i. Export Controls. The Software Product is specifically subject to the U.S. Export Administration Regulations. The Software Product and underlying information and technology may not be downloaded or otherwise exported or re-exported: (i) into, or to a national or resident of, any country listed in the U.S. Export Administrative Regulations or any other country to which the United States has embargoed goods; (ii) to anyone on the United States Treasury Department's list of Specially Designated Nations or the United States Commerce Department's Table of Denial Orders; or (iii) to any country or organization prohibited by any agency of the government of the United States. User acknowledges and agrees not to, directly or indirectly, resell, transfer disclose, export or re-export the Software Product in violation of the U.S. Export Administration Regulations (or any equivalent thereof) without the appropriate United States or foreign government licenses and/or authorizations.
 - j. U.S. Government Restricted Rights. The Software Product and documentation are "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFARS Section 227.7202 and FAR Section 12.212(b), Manufacturer is Skyline Technology Solutions, LLC, 6956 Aviation Boulevard, Glen Burnie, Maryland 21061. The Software Product and documentation was developed fully at private expense.
4. Confidential Information. Each party recognizes that this Agreement will allow it to come into possession of information that may comprise valuable trade secrets and other confidential information ("Confidential Information") which is exclusively owned by the other or by a third party. Each party expressly recognizes that such Confidential Information is being conveyed to the other under conditions of confidentiality, and agrees that it shall not use, for its own benefit or for the benefit of others, and shall not disclose Confidential Information belonging to the other or a third party to any third party during the term of this Agreement or at anytime after the termination of this Agreement.
 5. Report to Skyline. User recognizes that User's operation of the Software Product may result in the identification of defects and errors. The knowledge of these defects and errors may be

helpful to Skyline's continued development of the Software Product. User may voluntarily report to Skyline any defects or errors which User recognizes in the operation of the Software Product. This report to Skyline is strictly voluntary. Failure to report defects or errors to Skyline in no way terminates or alters User's duties under this Agreement unless the failure to correct said defects or errors renders the Software Product unusable, or unless the User is separately paying Skyline for a Software Support Agreement. In the exercise of its sole discretion and from time to time, Skyline may develop and make available maintenance releases for the Software Product. Such maintenance releases are made available at no cost to the User if User has a current annual support service agreement with Skyline.

6. **Warranties.** Skyline warrants that for a period of ninety (90) days from the point that User's system has gone live and User has accepted the Software Product, or until such time as the User terminates its Maintenance Services Agreement with Skyline, whichever is earlier, the Software Product substantially conforms to its published specifications. Skyline warrants that as delivered to User, the software does not contain any virus or programming that will cause the software to become inoperable or incapable of being used in accordance with its user manuals.

6.1 **Disclaimer of Warranties.** THE EXPRESS WARRANTY IN SECTION 6 ABOVE IS IN LIEU OF AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, SKYLINE AND ITS LICENSORS DISCLAIM, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE) REGARDING OR RELATING TO THE SOFTWARE, THE DOCUMENTATION, OR ANY MATERIALS FURNISHED OR PROVIDED TO YOU UNDER THIS AGREEMENT. SKYLINE AND ITS LICENSORS DO NOT WARRANT THAT THE SOFTWARE WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR THAT THE SOFTWARE WILL MEET (OR IS DESIGNED TO MEET) USER'S BUSINESS REQUIREMENTS.

7. **Disclaimers.** Except for any warranties set forth herein the Software Product provided by Skyline is provided, WITHOUT WARRANTY OF ANY KIND TO USER OR ANY THIRD PARTY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND UNDER THIS AGREEMENT. Except as it relates to the obligations of the Parties in Sections 8 and 9 below (Skyline and User Indemnification), Skyline's and User's aggregate liability whether for negligence, breach of warranty, or any other cause of action shall in no event exceed the price paid for the Software Product by the User to the Skyline. Skyline assumes no responsibility whatsoever for the performance of the User's computer hardware, operating systems, video sources or network connections. In no event does Skyline warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

8. **Skyline Indemnification.** Skyline shall indemnify, defend, and hold harmless User and its respective directors, officers, partners, members, employees and agents from and against all claims, damages, losses, liabilities, costs and expenses arising out of any claim solely by a third party:

- a. asserting that the Software Product or any User's use thereof pursuant to the terms of this Agreement, infringes such third party's patent, copyright, trademark, trade secret, confidentiality or other right, provided that User notifies Skyline in writing of the claim. Skyline's obligations under this

section shall not apply to the extent of any claim or infringement resulting from (i) User's continued use of the infringing product after receipt of notice from Skyline of a claim or after receipt of the remedy required of Skyline under this section; (ii) modifications to the Software Product by any party other than Skyline or its subcontractors or agents; (iii) modifications to the Software Product by Skyline made pursuant to User's express instructions and owned by User; (iv) combination of the Software Product with other products, processes or materials not provided by Skyline and not specified by the applicable documentation; or (v) User's use of the Software Product other than in accordance with the terms of this Agreement. If use of the Software Product is ever restricted or prohibited as a result of any such infringement, misappropriation or violation of another's rights, then Skyline shall, either (a) obtain for User the right to continue use of the Software Product as provided for in this Agreement; (b) modify the infringing Software Product to be non-infringing; (c) replace the Software Product with substantially similar software with at least the same functionality or (d) refund all fees paid by User under this Agreement for the current year; OR

b. Indemnification of costs and expenses shall extend only to actual costs and expenses assessed. Skyline's obligation to indemnify User as set forth above is conditioned on User giving Skyline prompt written notice of all claims, providing reasonable cooperation in their investigation and defense, and permitting Skyline to defend User at Skyline's expense with legal counsel of Skyline's choice.

9. **User's Indemnification.** To the extent permitted by applicable law, and as a condition for use of the Software Product, User hereby agrees that User will indemnify and hold harmless, Skyline, from any claims for damages or losses, brought against Skyline solely by third parties (not affiliates of User) arising from or related to use of the Software Product by User, or any related act or omission of User. User further agrees to indemnify Skyline against any award of damages and costs made against Skyline by a court of last resort arising from or related to any act or omission of User. Indemnification of costs shall extend only to actual costs assessed. User's obligation to indemnify Skyline as set forth above is conditioned on Skyline giving User prompt written notice of all claims, providing reasonable cooperation in their investigation and defense, and permitting User to defend Skyline at User's expense with legal counsel of User's choice.

10. **Entire Agreement.** This Agreement supersedes any and all other agreements, either oral or in writing, between the parties with respect to the matters stated herein, and this Agreement contains all the covenants and agreements between the parties with respect thereto. This Agreement may be amended or modified only in writing and shall be effective only after affixation of both parties' signatures.

11. **Knowing Consent and Authority to Consent.** The parties knowingly and expressly consent to the foregoing terms and conditions. Each party is authorized to enter into this Agreement on behalf of its respective party. The parties acknowledge that each party and its respective counsel have had an opportunity to review and revise this Agreement and that the normal rule of construction to the effect that any ambiguities are to be resolved against the drafting party shall not be employed in the interpretation of this Agreement or any amendments or exhibits, or schedules hereto.

12. **Miscellaneous.**

- a. Both parties agree that, except as may be required by applicable law or regulations, they shall not disclose in advertising, publicity or otherwise, the terms and conditions of this Agreement without prior written consent of the other party.
- b. This Agreement shall be construed in accordance with the laws of the State of Maryland, without regard for its conflicts of laws provisions. Both parties hereby submit to the exclusive jurisdiction of the state and Federal courts of the State of Maryland, for resolution of all disputes arising out of or related to the subject matter of this Agreement, and each agrees to waive their right to jury trial. Notwithstanding the foregoing, if User is a federal, state or local government agency or instrumentality, and if required by applicable law, this Agreement is governed by applicable laws of the U.S. state or territory in which User is located. Conflict of law rules are expressly disclaimed. To the extent that any terms and conditions in this Agreement are inconsistent with applicable laws of the U.S. state or territory in which User is located, those terms shall be deemed deleted and unenforceable.
- c. Each paragraph and provision are severable from the Agreement, and if one or more provisions or parts are declared invalid by a court of competent jurisdiction, the remaining provisions shall nevertheless remain in full force and effect. Any waiver (expressed or implied) or delay by either Party of any default or breach of this Agreement shall not constitute a waiver of any other or subsequent default or breach.
- d. Section Captions are inserted only for convenience and are in no way to be construed as part of this Agreement.
- e. Force Majeure. Except for User's payment obligations, neither party will be liable for any delay or failure to perform due to any cause beyond the party's reasonable control, including labor disputes, industrial disturbances, systemic utility failures, acts of nature, pandemics, embargoes, riots, government orders, acts of terrorism, or war.
- f. End-of-Life. Skyline reserves the right to discontinue the publication, sale, distribution, subscription, licensing, and support of any or all Software Products at any time and for any reason (each event herein "End-of-Life") by announcement or publication of notice to the general public or revision of its price list. Please refer to Skyline's then-current End-of-Life Policies and a then-current list of Software Products subject to an End-of-Life notice at <https://skylinenet.net/skyline-video-platform-lifecycle-policy/>. The Parties agree that an End-of-Life announcement of any Software Product shall not be considered a breach hereof by Skyline, nor shall any such End-of-Life entitle User to any claim for compensation or damages as result of or in connection therewith.



State of Minnesota Contract

SWIFT Contract Number: 252928

This Contract is between the State of Minnesota, acting through its Commissioner of Administration ("State") and RapidSOS, Inc., whose designated business address is 3 Park Avenue, 22nd Floor, New York, NY 10016 ("Contractor"). State and Contractor may be referred to jointly as "Parties."

Recitals

1. State issued a solicitation identified as G0210-2000015106 on November 18th, 2023 for 911 Automatic Location Identification (ALI) Solution ("Solicitation");
2. Contractor provided a response to the Solicitation indicating its interest in and ability to provide the goods or services requested in the Solicitation; and
3. Subsequent to an evaluation in accordance with the terms of the Solicitation, the Parties desire to enter into a contract.

Accordingly, the Parties agree as follows:

Contract

1. Term of Contract

- 1.1 Effective date. July 01, 2024, or the date the State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2, whichever is later. The Contractor must not begin work under this Contract until this Contract is fully executed and the Contractor has been notified by the State's Authorized Representative to begin the work.
- 1.2 Expiration date. July 31, 2026, or until all obligations have been satisfactorily fulfilled, whichever occurs first. The contract may be extended for up to an additional 60 months in increments as determined by the State, through a duly executed amendment.
- 1.3 Contract Use. This Contract is not exclusive and shall not be construed as guarantying a minimum or maximum amount of usage.

2. Contractor's Duties

The Contractor shall perform all duties described in this Contract to the satisfaction of the State.

3. Representations and Warranties

- 3.1 Under Minn. Stat. §§ 15.061 and 16C.03, subd. 3, and other applicable law the State is empowered to engage such assistance as deemed necessary.

3.2 Contractor warrants that it is duly qualified and shall perform its obligations under this Contract in accordance with the commercially reasonable standards of care, skill, and diligence in Contractor's industry, trade, or profession, and in accordance with the specifications set forth in this Contract, to the satisfaction of the State.

3.3 Contractor warrants that it possesses the legal authority to enter into this Contract and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Contract, or any part thereof, and to bind Contractor to its terms.

4. Time

The Contractor must comply with all the time requirements described in this Contract. In the performance of this Contract, time is of the essence.

5. Compensation and Conditions of Payment

5.1 Compensation. The State will pay for performance by the Contractor under this Contract in accordance with the breakdown of costs as set forth in Exhibit D which is attached and incorporated into this Contract.

5.2 Conditions of Payment. All duties performed by the Contractor under this Contract must be performed to the State's satisfaction and in accordance with all applicable federal, state, and local laws, ordinances, rules, and regulations including business registration requirements of the Office of the Secretary of State. The Contractor will not receive payment for work found by the State to be unsatisfactory or performed in violation of federal, state, or local law.

6. Authorized Representative

6.1 The State's Authorized Representative is Matt Hassenstab, Acquisition Management Specialist, Matt.Hassenstab@state.mn.us or his/her successor or delegate and has the responsibility to monitor the Contractor's performance.

6.2 Contractor's Authorized Representative. The Contractor's Authorized Representative is Chad Somodi, VP of Public Sector Sales, at the following business address and telephone number: 3 Park Avenue, 22nd Floor, New York, NY 10016 and 646-532-9775, or his/her successor. If the Contractor's Authorized Representative changes at any time during this Contract, the Contractor must immediately notify the State.

7. Exhibits

The following Exhibits are attached and incorporated into this Contract. In the event of a conflict between the terms of this Contract and its Exhibits, or between Exhibits, the order of precedence is first the Contract, and then in the following order:

Exhibit A: Contract Terms

Exhibit B: Insurance Requirements

Exhibit C: Specifications, Duties, and Scope of Work

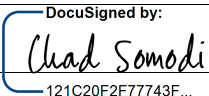
Exhibit D: Price and Payment Schedule

Exhibit E: RapidSOS EULA

1. Contractor
The Contractor certifies that the appropriate person(s) have executed the Contract on behalf of the Contractor as required by applicable articles, bylaws, resolutions, or ordinances.

Chad Somodi

Print name: _____

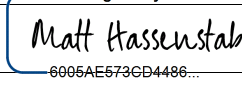
Signature:  DocuSigned by: 121C20F2F77743F... 8/13/2024

Title: VP of Sales Date: _____

2. State Agency
With delegated authority

Matt Hassenstab

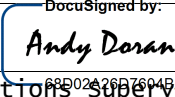
Print name: _____ DocuSigned by: _____

Signature:  6005AE573CD4486... 8/14/2024

Title: Acquisition Management Specialist Date: _____

3. Commissioner of Administration
As delegated to The Office of State Procurement
Andy Doran

Print name: _____ DocuSigned by: _____

Signature:  88D024285769484... IT Acquisitions Supervisor

Title: _____ Date: 8/14/2024

Exhibit A: Contract Terms

1. Prompt Payment and Invoicing.

- 1.1 Prompt Payment. The State will pay the Contractor pursuant to Minn. Stat. § 16A.124, which requires payment within 30 days following receipt of an undisputed invoice, or merchandise or service, whichever is later. Terms requesting payment in less than 30 days will be changed to read “Net 30 days.”
Notwithstanding the foregoing, the State may pay the Contractor in advance for purchases as allowed pursuant to Minn. Stat. §16A.065.

The payment for each order will only be made for goods received or services actually performed that have been accepted by the ordering entity, and meet all terms, conditions, and specifications of the Contract and the ordering document.

- 1.2 Invoicing. The invoice must be in the same format as the sample invoice form approved as Exhibit D, Supplement 1 with the Contract, unless an alternative format is approved in writing by the State Authorized Representative, or delegate. See Exhibit D, Supplement 1 for a list of minimum invoice requirements.

2. Assignment, Amendments, Waiver, and Contract Complete.

- 2.1 Assignment. The Contractor may neither assign nor transfer any rights or obligations under this Contract without the prior consent of the State and a fully executed assignment agreement, executed and approved by the authorized parties or their successors.
- 2.2 Amendments. Any amendment to this Contract must be in writing and will not be effective until it has been executed and approved by the authorized parties or their successors.
- 2.3 Waiver. If the State fails to enforce any provision of this Contract, that failure does not waive the provision or its right to enforce it.
- 2.4 Contract Complete. This Contract contains all negotiations and agreements between the State and the Contractor. No other understanding regarding this Contract, whether written or oral, may be used to bind either party.

3. Termination.

- 3.1 Termination for Convenience. The State or Commissioner of Administration may cancel this Contract at any time, with or without cause, upon 30 days’ written notice to the Contractor. Upon termination for convenience, the Contractor will be entitled to payment, determined on a pro rata basis, for services or goods satisfactorily performed or delivered.
- 3.2 Termination for Breach. If the Contractor fails to perform according to the contract terms and conditions, the State is authorized to immediately cancel the Contract or purchase order, or any portion of it, and may obtain replacement goods or services and charge the difference of costs to the defaulting Contractor. In the event of default, the State reserves the right to pursue any other remedy available by law. A Contractor may be removed from the vendors list, suspended or debarred from receiving a Contract for failure to comply with terms and conditions of the Contract, or for failure to pay the State for the cost incurred on the defaulted Contract.
- 3.3 Termination for Insufficient Funding. The State may immediately terminate this Contract if it does not obtain funding from the Minnesota Legislature, or other funding source; or if funding cannot be continued

at a level sufficient to allow for the payment of the services addressed within this Contract. Termination must be by written notice to the Contractor. The State is not obligated to pay for any services that are provided after notice and effective date of termination. However, the Contractor will be entitled to payment, determined on a pro rata basis, for services satisfactorily performed to the extent that dedicated funds are available. The State will not be assessed any penalty if the Contract is terminated because of the decision of the Minnesota Legislature, or other funding source, not to appropriate funds. The State must provide the Contractor notice of the lack of funding. This notice will be provided within a reasonable time of the State's receiving notice.

4. Force Majeure.

Neither party shall be responsible to the other or considered in default of its obligations within this Contract to the extent that performance of any such obligations is prevented or delayed by acts of God, war, riot, disruption of government, or other catastrophes beyond the reasonable control of the party unless the act or occurrence could have been reasonably foreseen and reasonable action could have been taken to prevent the delay or failure to perform. A party relying on this provision to excuse performance must provide the other party prompt written notice of the inability to perform and take all necessary steps to bring about performance as soon as practicable.

5. Indemnification.

5.1 In the performance of this Contract, the Indemnifying Party must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the State, to the extent caused by Indemnifying Party's:

- Intentional, willful, or negligent acts or omissions; or
- Actions that give rise to strict liability; or
- Breach of contract or warranty.

The Indemnifying Party is defined to include the Contractor, Contractor's reseller, any third party that has a business relationship with the Contractor, or Contractor's agents or employees, and to the fullest extent permitted by law. The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Indemnifying Party may have for the State's failure to fulfill its obligation under this Contract.

5.2 Nothing within this Contract, whether express or implied, shall be deemed to create an obligation on the part of the State to indemnify, defend, hold harmless or release the Indemnifying Party. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

6. Governing Law, Jurisdiction, and Venue.

Minnesota law, without regard to its choice-of-law provisions, governs this Contract. Venue for all legal proceedings out of this Contract, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

7. Contract Use by State Agencies.

To the extent applicable, the Contract does not prohibit state agencies from using their delegated purchasing authority to procure similar goods and services from other sources.

8. Warranty.

The Contractor warrants to the ordering entity that materials and equipment furnished under the Contract will be free from defects not inherent in the quality required or permitted, and that the work will conform to the requirements of the contract. Work not conforming to these requirements, including substitutions not properly approved and authorized

in writing may be considered defective. The Contractor's warranty excludes remedy for damage or defect caused by abuse, modifications not executed by the Contractor, improper or insufficient maintenance, improper operation, or normal wear and tear and normal usage. If requested, the Contractor shall furnish satisfactory evidence as to the kind and quality of materials and equipment used.

All installation materials and labor shall be guaranteed for a period of one (1) year following the date of final acceptance. During the first year following acceptance, the Contractor shall, upon notification by the ordering entity of any malfunctions, make necessary repairs, including labor, travel, and materials, at the Contractor's expense.

9. Original Equipment Manufacturer (OEM Warranty).

The equipment offered must include the OEM standard warranty. The Contractor is responsible for the cost of any inspections, adjustments, warranted parts, and labor charges to repair or replace warranted parts that are a result of equipment failure(s) during the warranty period. This shall be performed promptly unless otherwise mutually agreed in writing by the Customer and the Contractor. This warranty shall commence when the unit is put into service.

9.1 OEM Extended Warranty Options. If the Contractor provides an OEM Extended Warranty Option, the Contractor must provide a copy of the applicable terms and conditions, including a detail of coverage, to the State upon request. The cost of an OEM Extended Warranty must include all associated costs.

9.2 Contractor (Add-On) Warranty Options. The Contractor may provide additional warranty options, which include, but are not limited to travel pickup, or delivery charges that are a result of equipment failure(s) prior to or during the warranty period or extended warranty period. This warranty option shall commence when the unit is put into service and is in addition to OEM warranty options stated above.

10. Delivery.

Contractor is obligated to deliver within the quoted lead times. If delivery is not made within that time frame, the State reserves the right to deem the Contractor in default.

Contractor must confirm delivery locations and requirements with the ordering entity. Prior to delivery, the Contractor is responsible for confirming in writing with the ordering entity that the delivery location will accommodate unloading the equipment. Contractor must notify the receiving entity at least 72 hours before delivery to allow for inspection and compliance. No delivery can be made on a State Holiday (as defined in Minn. Stat. § 645.44, subd. 5), on Saturday or Sunday, or after 4:00 p.m. Central Time on weekdays, without prior written approval by the receiving entity.

11. Risk of Loss.

The State is relieved of all risks of loss or damage to the goods and equipment during periods of transportation, installation by the Contractor, or while in the possession of the Contractor or its agent.

12. Purchase Orders.

The parties agree that there is no minimum order requirements or charges to process an individual purchase order unless otherwise stated in the Contract. The Purchase Order number must appear on all documents (e.g., invoices, packing slips, etc.).

13. Equipment Specifications.

All equipment must meet the contract specifications and all federal and State safety codes and regulations in effect at the date of manufacture. All equipment must be Original Equipment Manufacturer (OEM) equipment unless otherwise stated in the contract.

14. Items Offered as New.

All products, materials, supplies, replacement parts, and equipment offered and furnished must be new, of current manufacturer production, and must have been formally announced by the manufacturer as being commercially available, unless otherwise stated in this Contract.

15. Subcontracting and Subcontractor Payment.

- 15.1 Subcontracting Allowed. A subcontractor is a person or company that has been awarded a portion of the Contract by Contractor. Only subcontractors that have been approved by the State's Authorized Representative can be used for this Contract.

After the effective date of the Contract, the Contractor shall not, without prior written approval of the State's Authorized Representative, subcontract for the performance of any of the Contractor's obligations that were not already approved for subcontracting when the Contract was awarded. During this Contract, if an approved subcontractor is determined to be performing unsatisfactorily by the State's Authorized Representative, the Contractor will receive written notification that the subcontractor can no longer be used for this Contract.

The provisions of the Contract shall apply with equal force and effect to all approved subcontractors engaged by the Contractor. Notwithstanding approval by the State, no subcontract shall serve to terminate or in any way affect the primary legal responsibility of the Contractor for timely and satisfactory performances of the obligations contemplated by the Contract.

- 15.2 Subcontractor Payment. Contractor must pay any subcontractor in accordance with Minn. Stat. § 16A.1245.

4. Data Disclosure.

Under Minn. Stat. § 270C.65, subd. 3 and other applicable law, the Contractor consents to disclosure of its social security number, federal employer tax identification number, and Minnesota tax identification number, already provided to the State, to federal and state agencies, and state personnel involved in the payment of state obligations. These identification numbers may be used in the enforcement of federal and state laws which could result in action requiring the Contractor to file state tax returns, pay delinquent state tax liabilities, if any, or pay other state liabilities.

16. Government Data Practices.

The Contractor and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (or, if the State contracting party is part of the Judicial Branch, with the Rules of Public Access to Records of the Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by the State under this Contract, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the Contractor under this Contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. Ch. 13, by either the Contractor or the State.

If the Contractor receives a request to release the data referred to in this clause, the Contractor must immediately notify and consult with the State's Authorized Representative as to how the Contractor should respond to the request. The Contractor's response to the request shall comply with applicable law.

17. Intellectual Property Rights.

- 17.1 Definitions. For the purpose of this Section, the following words and phrases have the assigned definitions:

17.1.1 “Documents” are the originals of any reports, whether in tangible or electronic forms, prepared by the Contractor, its employees, agents, or subcontractors, in the performance of this Contract and delivered to the State.

17.1.2 “Pre-Existing Intellectual Property” means intellectual property developed prior to or outside the scope of this Contract, and any derivatives of that intellectual property.

17.1.3 “Works” means all inventions, improvements, discoveries (whether or not patentable), databases, computer programs, reports, notes, studies, photographs, negatives, designs, drawings, specifications, materials, tapes, and disks conceived, reduced to practice, created or originated by the Contractor, its employees, agents, and subcontractors, either individually or jointly with others in the performance of this Contract. “Works” includes Documents.

17.2 Ownership. The State is hereby granted a limited right to use the Works and Documents created by Contractor and paid for under this Contract during the term of this Contract and shall have the right to continue to use the Documents after the expiration of the Contract. All portions of the Works and Documents that contain the State’s confidential and/or proprietary information shall be the exclusive property of the State. In no event shall any of the Works under this Contract be deemed to be “works made for hire.”

17.3 Pre-existing Intellectual Property. Each Party shall retain ownership of its respective Pre-Existing Intellectual Property, including any improvements thereto. The Contractor grants the State rights to use Contractor’s Pre-Existing Intellectual Property that are incorporated in the products, materials, equipment, deliverables, or services that are purchased through the Contract during the term of the Contract. Upon termination of the Contract, all rights of use in Contractor’s Pre-existing Intellectual Property, including any improvements thereto, shall automatically terminate.

17.4 Obligations.

17.4.1 Notification. Whenever any invention, improvement, or discovery (whether or not patentable) is made or conceived for the first time or actually or constructively reduced to practice by the Contractor, including its employees and subcontractors, in the performance of this Contract, the Contractor will immediately give the State’s Authorized Representative written notice thereof, and must promptly furnish the State’s Authorized Representative with complete information and/or disclosure thereon.

17.4.2 Representation. The Contractor must perform all acts, and take all steps necessary to ensure that all intellectual property rights in the Works and Documents are the sole property of the State, and that neither Contractor nor its employees, agents, or subcontractors retain any interest in and to the Works and Documents. The Contractor represents and warrants that the Works and Documents do not and will not infringe upon any intellectual property rights of other persons or entities.

17.4.3 Indemnification. Notwithstanding any other indemnification obligations addressed within this Contract, the Contractor will indemnify; defend, to the extent permitted by the Attorney General; and hold harmless the State, at the Contractor’s expense, from any action or claim brought against the State to the

extent that it is based on a claim that all or part of the Works or Documents infringe upon the intellectual property rights of others. The Contractor will be responsible for payment of any and all such claims, demands, obligations, liabilities, costs, and damages, including but not limited to, attorney fees. If such a claim or action arises, or in the Contractor's or the State's opinion is likely to arise, the Contractor must, at the State's discretion, either procure for the State the right or license to use the intellectual property rights at issue or replace or modify the allegedly infringing works or documents as necessary and appropriate to obviate the infringement claim. This remedy of the State will be in addition to and not exclusive of other remedies provided by law.

18. Copyright.

The Contractor shall save and hold harmless the State of Minnesota, its officers, agents, servants and employees, from liability, arising from the use of any copyrighted or noncopyrighted compositions, secret process, patented or nonpatented invention, article or appliance furnished by Contractor and used in the performance of the Contract during the term of the Contract.

19. Assignment of Antitrust Rights.

Upon the request of the State of Minnesota, Contractor will irrevocably assign to State any state or federal antitrust claim or cause of action that the Contractor now has or which may accrue to the Contractor in the future, in connection with any goods, services, or combination provided by Contractor under the terms of this Contract.

20. Survivability of Orders.

In the event the term of any order or Professional/Technical Services work order ("Order") placed under this Contract extends past the termination or expiration of this Contract, the terms and conditions of this Contract shall remain in full force and effect as it applies to such order and will continue in effect for such order until the term of that order expires or the order is cancelled or terminated in accordance with the terms of this Contract.

21. Contractor's Documents.

Any licensing and maintenance agreement, or any order-specific agreement or document, including any pre-installation, linked or "click through" agreement that is allowed by, referenced within or incorporated within the Contract whenever the Contract is used for a State procurement, whether directly by the Contractor or through a Contractor's agent, subcontractor or reseller, is agreed to only to the extent the terms within any such agreement or document do not conflict with the Contract or applicable Minnesota or Federal law, and only to the extent that the terms do not modify, diminish or derogate the terms of the Contract or create an additional financial obligation to the State. Any such agreement or document must not be construed to deprive the State of its sovereign immunity, or of any legal requirements, prohibitions, protections, exclusions or limitations of liability applicable to this Contract or afforded to the State by Minnesota law. A State employee's decision to choose "accept" or an equivalent option associated with a "click-through" agreement does not constitute the State's concurrence or acceptance of terms, if such terms are in conflict with this section.

22. State Audits.

Under Minn. Stat. § 16C.05, subd. 5, the Contractor's books, records, documents, and accounting procedures and practices relevant to this Contract are subject to examination by the State, the State Auditor, or Legislative Auditor, as appropriate, for a minimum of six years from the expiration or termination of this Contract.

23. Usage Reports.

Contractor must track and report to the State usage data on this Contract (Usage Reports). Usage Reports should be sent via email to osp.usagereports@state.mn.us. A Usage Report must identify the State Contract Number and provide the following information:

- The total amount of spend under the Contract by the State and other entities,
- The total amount of spend by State agencies, and
- The total amount of spend by other entities (CPV members).

Contractor must send a quarterly Usage Report, or as otherwise requested. Quarters are as follows:

- First Quarter, from July 1 to September 30,
- Second Quarter, from October 1 to December 31,
- Third Quarter, from January 1 to March 31, and
- Fourth Quarter, from April 1 to June 30.

A quarterly Usage Report is due within thirty days of the end of a quarter. A requested Usage Report is due within thirty days from when the request was made. Contractor must provide the State with a final Usage Report within 30 calendar days of the expiration or termination of the Contract. Failure to provide a Usage Report may result in the State cancelling the Contract. This term survives the expiration or termination of the Contract.

24. Diverse Spend Reporting.

If the total value of the Contract may exceed \$500,000, including all extension options, Contractor must track and report, on a quarterly basis, the amount paid to diverse businesses both: 1) directly to subcontractors performing under the Contract, and 2) indirectly to diverse businesses that provide supplies/services to your company (in proportion to the revenue from this Contract compared to Contractor's overall revenue). When this applies, Contractor will register in a free portal to help report the Tier 2 diverse spend, and the requirement continues as long as the Contract is in effect.

25. Publicity and Endorsement.

25.1 Publicity. Any publicity regarding the subject matter of this Contract must identify the State as the sponsoring agency and must not be released without prior written approval from the State's Authorized Representative. For purposes of this provision, publicity includes notices, informational pamphlets, press releases, information posted on corporate or other websites, research, reports, signs, and similar public notices prepared by or for the Contractor individually or jointly with others, or any subcontractors, with respect to the program, publications, or services provided resulting from this Contract.

25.2 Endorsement. The Contractor must not claim that the State endorses its products or services.

26. Debarment by State, its Departments, Commissions, Agencies, or Political Subdivisions.

Contractor certifies that neither it nor its principals is presently debarred or suspended by the Federal government, the State, or any of the State's departments, commissions, agencies, or political subdivisions. Contractor's certification is a material representation upon which the Contract award was based. Contractor shall provide immediate written notice to the State's Authorized Representative if at any time it learns that this certification was erroneous when submitted or becomes erroneous by reason of changed circumstances.

27. Contingency Fees Prohibited.

Pursuant to Minn. Stat. § 10A.06, no person may act as or employ a lobbyist for compensation that is dependent upon the result or outcome of any legislation or administrative action.

28. Certification of Nondiscrimination (in accordance with Minn. Stat. § 16C.053).

If the value of this Contract, including all extensions, is \$50,000 or more, Contractor certifies it does not engage in and has no present plans to engage in discrimination against Israel, or against persons or entities doing business in Israel, when making decisions related to the operation of the vendor's business. For purposes of this section, "discrimination" includes but is not limited to engaging in refusals to deal, terminating business activities, or other actions that are intended to limit commercial relations with Israel, or persons or entities doing business in Israel, when such actions are

taken in a manner that in any way discriminates on the basis of nationality or national origin and is not based on a valid business reason.

29. Non-discrimination (in accordance with Minn. Stat. § 181.59).

The Contractor will comply with the provisions of Minn. Stat. § 181.59.

30. E-Verify Certification (in accordance with Minn. Stat. § 16C.075).

For services valued in excess of \$50,000, Contractor certifies that as of the date of services performed on behalf of the State, Contractor and all its subcontractors will have implemented or be in the process of implementing the federal E-Verify Program for all newly hired employees in the United States who will perform work on behalf of the State. Contractor is responsible for collecting all subcontractor certifications and may do so utilizing the [E-Verify Subcontractor Certification Form](#). All subcontractor certifications must be kept on file with Contractor and made available to the State upon request.

31. Affirmative Action Requirements

The State intends to carry out its responsibility for requiring affirmative action by its contractors.

- 31.1 Covered Contracts and Contractors. If the Contract exceeds \$100,000 and the Contractor employed 40 or more full-time employees on a single working day during the previous 12 months in Minnesota or in the state where it has its principal place of business, then the Contractor must comply with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600.
- 31.2 General. Minn. R. 5000.3400-5000.3600 implements Minn. Stat. § 363A.36. These rules include, but are not limited to, criteria for contents, approval, and implementation of affirmative action plans; procedures for issuing certificates of compliance and criteria for determining a contractor's compliance status; procedures for addressing deficiencies, sanctions, and notice and hearing; annual compliance reports; procedures for compliance review; and contract consequences for non-compliance. The specific criteria for approval or rejection of an affirmative action plan are contained in various provisions of Minn. R. 5000.3400-5000.3600 including, but not limited to, Minn. R. 5000.3420-5000.3500 and 5000.3552-5000.3559.
- 31.3 Disabled Workers. The Contractor must comply with the following affirmative action requirements for disabled workers.

AFFIRMATIVE ACTION FOR DISABLED WORKERS

- 31.3.1 The Contractor must not discriminate against any employee or applicant for employment because of physical or mental disability in regard to any position for which the employee or applicant for employment is qualified. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified disabled persons without discrimination based upon their physical or mental disability in all employment practices such as the following: employment, upgrading, demotion or transfer, recruitment, advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.
- 31.3.2 The Contractor agrees to comply with the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.
- 31.3.3 In the event of the Contractor's noncompliance with the requirements of this clause, actions for noncompliance may be taken in accordance with Minn. Stat. § 363A.36, and the rules and relevant orders of the Minnesota Department of Human Rights issued pursuant to the Minnesota Human Rights Act.

31.3.4 The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices in a form to be prescribed by the Commissioner. Such notices must state the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified disabled employees and applicants for employment, and the rights of applicants and employees.

31.3.5 The Contractor must notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of Minn. Stat. § 363A.36, of the Minnesota Human Rights Act and is committed to take affirmative action to employ and advance in employment physically and mentally disabled persons.

31.4 Consequences. The consequences for the Contractor's failure to implement its affirmative action plan or make a good faith effort to do so include, but are not limited to, suspension or revocation of a certificate of compliance by the Commissioner, refusal by the Commissioner to approve subsequent plans, and termination of all or part of this Contract by the Commissioner or the State.

31.5 Certification. The Contractor hereby certifies that it is in compliance with the requirements of Minn. Stat. § 363A.36 and Minn. R. 5000.3400-5000.3600 and is aware of the consequences for noncompliance.

32. Equal Pay Certification.

If required by Minn. Stat. §363A.44, the Contractor must have a current Equal Pay Certificate prior to Contract execution. If Contractor's Equal Pay Certificate expires during the term of this Contract, Contractor must promptly re-apply for an Equal Pay Certificate with the Minnesota Department of Human Rights and notify the State's Authorized Representative once the Contractor has received the renewed Equal Pay Certificate. If Contractor claims to be exempt, the State may require Contractor to verify its exempt status.

33. Professional/Technical (P/T) Services Ancillary to Goods or General Services.

For state agencies, Professional/Technical (P/T) Services must be related to the goods or services purchased from this Contract and is limited to \$50,000 per project. Based on the size, scope and complexity of a project, the State's Authorized Representative may approve dollar limits exceeding \$50,000 per project. This may require a separate work order contract defining the PT scope of work.

Ten percent (10%) of the cost of each P/T deliverable will be withheld by the State. The retainage will be held by the State until the P/T deliverable has been reviewed by the head of the agency entering into the Contract and the head of the agency has certified that the Contractor has satisfactorily fulfilled the terms of the Contract.

34. Hazardous Substances.

To the extent that the goods to be supplied to the State by the Contractor contain or may create hazardous substances, harmful physical agents, or infectious agents, as set forth in applicable State and federal laws and regulations, the Contractor must provide the State with Material Safety Data Sheets regarding those substances. A copy must be provided upon request. Goods and containers supplied to the State must be labeled in compliance with state and federal laws, rules, and regulations.

These terms apply to goods supplied under this contract:

34.1 Products Containing Triclosan Banned. The Contractor must comply with Minn. Stat. § 145.945.

34.2 Products Containing Certain Types of Polybrominated Diphenyl Ether Banned. The Contractor must comply with Minn. Stat. § 325E.385-325E.388).

34.3 Coal Tar Sealant Use and Sale Prohibited. The Contractor must comply with Minn. Stat. § 116.202.

34.4 Products Containing Mercury. The Contractor must comply with Minn. Stat. 116.92.

35. IT Accessibility Standard.

Contractor acknowledges and is fully aware that the State of Minnesota (Executive branch state agencies) has developed its IT Accessibility Standard effective September 1, 2010. The Standard entails, in part, the Web Content Accessibility Guidelines (WCAG) and Section 508 which can be viewed at: <https://mn.gov/mnit/government/policies/accessibility/>.

The Standard applies to web sites, software applications, electronic reports and output documentation, training delivered in electronic formats (including, but not limited to, documents, videos, and webinars), among others. As upgrades are made to the software, products, or subscriptions available through this Contract, the Contractor agrees to develop functionality which supports accessibility. If any issues arise due to nonconformance with the above-mentioned accessibility Standard, the Contractor agrees to provide alternative solutions upon request at no additional charge to the State.

When updates or upgrades are made to the products or services available through this Contract, the Contractor agrees to document how the changes will impact or improve the product or service's accessibility and usability. This documentation, upon request, must be provided to the State in advance of the change, occurring within an agreed upon timeframe sufficient for the state to review the changes and either approve them or request a remediation plan from the Contractor. Contractor warrants that its Products comply with the above-mentioned accessibility Standards and agrees to indemnify, defend, and hold harmless the State against any claims related to non-compliance of Contractor's Product with the above-mentioned accessibility Standard. If agreed-upon updates fail to improve the product or service's accessibility or usability as planned, the failure to comply with this requirement may be cause for contract cancellation or for the State to consider the Contractor in default.

36. Security and Data Protection.

Contractor is responsible for the security and protection of State data subject to and related to Cloud Services in this Contract. The terms, conditions, and provisions of this Security and Data Protection section take precedence and will prevail over any other terms, conditions, and provisions of the Contract, if in conflict. This Security and Data Protection section, including its sub-sections, survives the completion, termination, expiration, or cancellation of the Contract.

36.1 For the purposes of this Security and Data Protection section, the following terms have the following meanings:

36.1.1 "Cloud Services" includes "cloud computing" as defined by the U.S. Department of Commerce, NIST Special Publication 800-145 (currently available online at: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>) and any other software, hardware, hosting service, subscription, or other service or product by which Contractor stores, transmits, processes or otherwise has access to State data.

36.1.2 "State" means the State, or a cooperative purchasing venture ("CPV") member when the CPV member is the ordering entity (if CPV purchases are permitted under this Contract).

36.1.3 "Data" has the meaning of "government data" in Minn. Stat. § 13.02, subd. 7.

36.1.4 "Not public data" has the meaning in Minn. Stat. § 13.02, subd. 8a.

36.1.5 "Security incident" means any actual, successful or suspected: (1) improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, modification of, alteration

to, loss of, damage to or destruction of State data; (2) interference with an information system; (3) disruption of or to Contractor's service(s); or (4) any similar or related incident.

36.1.6 "Privacy incident" means violation of the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); violation of federal data disclosure or privacy requirements in federal laws, rules and regulations; or breach of a contractual obligation to protect State data. This includes, but is not limited to, improper or unauthorized access to, viewing of, obtaining of, acquisition of, use of, disclosure of, damage to, loss of, modification of, alteration to or destruction of State data protected by such State or federal laws or by contract.

36.2 Data Ownership. The State solely and exclusively owns and retains all right, title and interest, whether express or implied, in and to any and all State data. Contractor has no and acquires no right, title or interest, whether express or implied, in and to State data.

Contractor will only use State data for the purposes set forth in the Contract. Contractor will only access State data as necessary for performance of this Contract. Contractor will not access State user accounts except to respond to service or technical problems or at the State's specific request.

All State data, including copies, summaries and derivative works thereof, must be remitted, in a mutually agreeable format and media, to the State by the Contractor upon request or upon completion, termination or cancellation of the Contract. The foregoing sentence does not apply if the State Chief Information Security Officer or delegate authorizes in writing the Contractor to sanitize or destroy the data and the Contractor certifies in writing the sanitization or destruction of the data. Within ninety days following any remittance of State data to the State, Contractor shall, unless otherwise instructed by the State in writing, sanitize or destroy any remaining data and certify in writing that the sanitization or destruction of the data has occurred. Any such remittance, sanitization or destruction will be at the Contractor's sole cost and expense.

In the event Contractor receives a request to release any State data, Contractor must immediately notify the State's data practices compliance official. The State will give Contractor instructions concerning the release of the data to the requesting party before the data is released. Contractor must comply with the State's instructions. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data by Contractor.

36.3 Notification of Incidents. If Contractor becomes aware of or has reasonable suspicion of a privacy incident or security incident regarding any State data, Contractor must report such incident to the State and the State Chief Information Security Officer as soon as possible, but no later than twenty-four (24) hours after such incident. The decision to notify the affected data subjects and the form of such notice following report of a privacy incident or security incident are the responsibility of the State. Notwithstanding anything to the contrary in this Contract, Contractor will indemnify, hold harmless and defend the State and its officers, and employees for and against any claims, damages, costs and expenses related to any privacy incident or security incident involving any State data. For purposes of clarification, the foregoing sentence shall in no way limit or diminish Contractor's obligation(s) to indemnify, save, hold harmless, or defend the State under any other term of this Contract. Contractor will reasonably mitigate any harmful effects resulting from any privacy incident or security incident involving any State data.

36.4 Security Program. Contractor will make best efforts to protect and secure the State data related to this Contract. Contractor will establish and maintain an Information Security Program ("Program") that includes an information security policy applicable to any and all Cloud Services ("Policy"). Contractor's Program and Policy must align with appropriate industry security frameworks and standards such as National Institute of Standards and Technology ("NIST") 800-53 Special Publication Revision 5, Federal Information Processing Standards ("FIPS") 199, Federal Risk and Authorization Management Program ("FedRamp"), or Control Objectives for Information and Related Technology ("COBIT").

Upon the State's request, Contractor will make its Policy available to the State on a confidential, need-to-know basis, along with other related information reasonably requested by the State regarding Contractor's security practices and policies. Unless inconsistent with applicable laws, Contractor and the State must treat the Policy and related information on security practices and policies that are specific to the State as confidential information and as not public data pursuant to Minn. Stat. § 13.37.

- 36.5 Data Management. Contractor will not use State data, including production data, for testing or development purposes unless authorized in writing by the State Chief Information Security Officer or delegate. Contractor will implement and maintain procedures to physically and logically segregate State data, unless otherwise explicitly authorized by the State Chief Information Security Officer or delegate.
- 36.6 Data Encryption. Contractor must encrypt all State data at rest and in transit, in compliance with FIPS Publication 140-2 or applicable law, regulation or rule, whichever is a higher standard. All encryption keys must be unique to State data. Contractor will secure and protect all encryption keys to State data. Encryption keys to State data will only be accessed by Contractor as necessary for performance of this Contract.
- 36.7 Data Storage. Contractor warrants that any and all State data will be stored, processed, and maintained solely on designated servers and that no such data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is in use as part of the Contractor's designated backup and recovery processes.
- 36.8 Data Center and Monitoring/Support Locations. During the term of the Contract, Contractor will: (1) locate all production and disaster recovery data centers that store, process or transmit State data only in the continental United States and Canada if applicable to the operations of the solution, (2) store, process and transmit State data only in the continental United States and Canada if applicable to the operations of the solution, and (3) locate all monitoring and support of all Cloud Services only in the continental United States and Canada if applicable to the operations of the solution. The State has the right to on-site visits and reasonable inspection of the data centers upon notice to Contractor of seven calendar days prior to visit.
- 36.9 Security Audits & Remediation. Contractor will audit the security of the systems and processes used to provide any and all Cloud Services, including those of the data centers used by Contractor to provide any and all Cloud Services to the State. This security audit: (1) will be performed at least once every calendar year beginning with 2016; (2) will be performed according Statement on Standards for Attestation Engagements ("SSAE") 16 Service Organization Control ("SOC") 2, International Organization for Standardization ("ISO") 27001, or FedRAMP; (3) will be performed by third party security professionals at Contractor's election and expense; (4) will result in the generation of an audit report ("Contractor Audit Report"), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13); and (5) may be performed for other purposes in addition to satisfying this section.

Upon the State's reasonable, advance written request, Contractor will provide to the State a copy of the Contractor Audit Report.

Contractor will make best efforts to remediate any control deficiencies identified in the Contractor Audit Report in a commercially reasonable timeframe.

If the State becomes aware of any other Contractor controls that do not substantially meet the State's requirements, the State may request remediation from Contractor. Contractor will make best efforts to remediate any control deficiencies identified by the State or known by Contractor, in a commercially reasonable timeframe.

36.10 Insurance and Liability. Contractor warrants that it has and will maintain the insurance described below in force and effect throughout the term of the Contract. An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor's policy limits to satisfy the full policy limits required by the Contract provided that Contractor warrants that the minimum coverage requirements below are met.

Professional/Technical, Errors and Omissions, including Network Security and Privacy Liability Insurance (or equivalent Network Security and Privacy Liability coverage endorsed on another form of liability coverage or written as a standalone policy):

This policy must provide coverage for all claims Contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to the Contract, including but not limited to claims which may arise from failure of Contractor's or a subcontractor's security resulting in, but not limited to, computer attacks, unauthorized access, disclosure of confidential or private information, transmission of a computer virus or denial of service.

Contractor is required to carry the following minimum limits:

\$2,000,000 – per claim or event
\$2,000,000 – annual aggregate

Any deductible will be the sole responsibility of the Contractor and, unless Contractor maintains an audited net worth of at least \$100 million, the deductible may not exceed \$100,000 without the written approval of the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources. The retroactive or prior acts date of such coverage shall not be after the effective date of the Contract. Contractor shall maintain such insurance for a period of at least three (3) years following expiration or termination of the Contract. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract. If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor will notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State. Contractor is responsible for payment of Contract related insurance premiums and deductibles. If Contractor is self-insured, a Certificate of Self-Insurance must be provided to the State. Contractor shall obtain insurance policy(ies) from insurance company(ies) having an "AM BEST" rating of A- (minus); Financial Size Category ("FSC") VII or better, and authorized to do business in the State. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's authorized representative upon written request. The State reserves the right to immediately terminate the Contract if the Contractor is not in compliance with the insurance requirements of this sub-section and retains all rights to pursue any legal remedies against the Contractor.

Notwithstanding any limitation of liabilities in the Contract, the Contractor shall be liable for all damages to the extent such damages are within the insurance limit.

36.11 Subcontractors and Third Parties. Contractor warrants that no State data will be transmitted, exchanged or otherwise provided to other parties except as specifically agreed to in writing by the State Chief Information Security Officer or delegate. Contractor must ensure that any contractors, subcontractors, agents and others to whom it provides State data, agree in writing to be bound by the same restrictions and conditions under this Contract that apply to Contractor with respect to such data.

36.12 Compliance with Data Privacy and Security Laws and Standards. Contractor shall comply with all applicable State and federal data privacy and data security laws, rules, and regulations.

36.13 Remedies. Contractor acknowledges that the State, because of the unique nature of its data, would suffer irreparable harm in the event that Contractor breaches its obligation under this Security and Data Protection section, and monetary damages may not adequately compensate the State for such a breach. In such circumstances, the State will be entitled, in addition to monetary relief, to injunctive relief or specific performance as may be necessary to restrain any continuing or further breach by Contractor, without showing or proving any actual damages sustained by the State.

36.14 Business Continuity. Contractor shall have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that Cloud Services provided under this Contract shall be maintained continuously in the event of a disruption to the Contractor's operations, regardless of the cause of the disruption. Such plans must, at a minimum, define the Contractor's actions to address the impacts of the following key areas likely to cause a disruption to Contractor's operations: loss of key personnel, loss of facility, and loss of information technology. Contractor must conduct testing and review of its business continuity and disaster recovery plan at least annually. Upon State request, Contractor must also participate, at mutually agreed upon times, in State business continuity and disaster recovery testing, training, and exercise activities.

Any term or condition that allows the Contractor to terminate the Contract for any or no reason (i.e., termination for convenience) is null and void. In the event of termination or cancellation of this Contract for any reason, the Contractor shall continue to provide any then-existing Cloud Services for as long as the State needs to transfer its data, software and other assets to an alternate service or service provider. After any such termination or cancellation, the State may purchase the continuing Cloud Services at the pricing in effect prior to such termination or cancellation. The fee for any such purchase shall be prorated for the period of time needed, as determined by the State, and shall be reduced by the amount paid for Cloud Services that were not used prior to such termination or cancellation. The amount of any such fee reduction shall be determined on a pro-rata basis. The Contractor shall refund to the State any unused portion of payments for Cloud Services.

36.15 Background Checks. Contractor represents that it has conducted and will conduct background investigations into all of Contractor's agents, employees, and subcontractors that will provide Cloud Services to the State. Such background investigations must have been or will be conducted by investigating local, state and federal criminal records, local, state and federal civil case records, and employment references.

If any provision of this sub-section is found to violate any applicable laws, rules, or State policies, then the Contractor will be relieved of all obligations arising under such provision. Notwithstanding anything to the contrary in this sub-section, this sub-section is only applicable and effective to extent that it is consistent with applicable laws, rules, and State policies.

36.16 Secure Coding. Contractor warrants that all Cloud Services are free from any and all defects in materials, workmanship, and design. Contractor warrants that all Cloud Services are free from any and all viruses, malware, and other harmful or malicious code. Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made and again before being placed into production, and must promptly remediate any and all vulnerabilities. Contractor must follow best practices for application code review and the most current version of the OWASP top 10.

36.17 Compliance with Data Privacy and Security Laws and Standards. Contractor shall comply with the applicable State of Minnesota Information Security Policy & Standards incorporated herein by reference and available at <https://mn.gov/mnit/government/policies/security/>.

Contractor shall comply with the Health Insurance Portability Accountability Act ("HIPAA"), the HITECH Act, and other similar privacy laws. Contractor also shall comply with the HIPAA Privacy Rule, HIPAA Security Rule, and other similar rules, regulations, and laws, including future amendments thereto.

Contractor acknowledges that for the purposes of this Contract when storing, processing, transmitting or otherwise accessing State data subject to the Family Educational Rights and Privacy Act ("FERPA"), it is designated as a "school official" with "legitimate educational interests" in State data and associated metadata, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Contractor shall use State data only for the purpose of fulfilling its duties under the Contract and it will not monitor or share such data with or disclose it to any third party except as provided for in this Contract, as required by law, or as authorized in writing by the State. By way of illustration and not of limitation, Contractor will not use such data for Contractor's own benefit and, in particular, will not engage in "data mining" of such data or communications, whether through automated or human means, except as necessary to fulfill its duties under this Contract, or as specifically and expressly provided for in this Contract, as required by law, or authorized in writing by the State. Contractor agrees, upon request, to provide the State with a written summary of the procedures Contractor uses to safeguard State data.

All of Contractor's systems and components that process, store, or transmit Cardholder Data shall comply with the most recent version of the Payment Card Industry Data Security Standard ("PCI DSS") promulgated by the PCI Security Standards Council, currently available online at: https://www.pcisecuritystandards.org/document_library. The Contractor shall, upon request, provide the State with Contractor's current Attestation of Compliance signed by a PCI QSA ("Qualified Security Assessor"). For purposes of this sub-section, "Cardholder Data" has the meaning defined by the PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), Glossary of Terms, Abbreviations, and Acronyms, currently available online at: https://www.pcisecuritystandards.org/document_library.

Contractor shall comply with IRS Publication 1075, Exhibit 7, which is incorporated herein.

For the term of this Contract, Contractor will maintain a provisional Authority to Operate (ATO) at the Moderate Level from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) or Federal Agency for any and all Cloud Services provided under this Contract.

For the term of this Contract, Contractor will maintain an ISO 27001 Certification for any and all Cloud Services provided under this Contract.

37. Survival of Terms.

The following clauses survive the expiration or cancellation of this Contract: Indemnification; State Audits; Government Data Practices; Intellectual Property; Publicity and Endorsement; Governing Law, Jurisdiction, and Venue; and Data Disclosure. Any other Contract term that expressly states or by its nature shall survive, shall survive.

Exhibit B: Insurance Requirements

1. Notice to Contractor.

- 1.1 The Contractor is required to submit Certificates of Insurance acceptable to the State as evidence of insurance coverage requirements prior to commencing work under this Contract.
- 1.2 The Contractor shall not commence work under the contract until they have obtained all the insurance described below and the State has approved such insurance. Contractor shall maintain such insurance in force and effect throughout the term of this Contract, unless otherwise specified in this Contract
- 1.3 The failure of the Contractor to provide a Certificate of Insurance, for the policies required under this Contract or renewals thereof, or failure of the insurance company to notify the State of the cancellation of policies required under this Contract shall not constitute a waiver by the State to the Contractor to provide such insurance.
- 1.4 The State reserves the right to immediately terminate this Contract if the Contractor is not in compliance with the insurance requirements and retains all rights to pursue any legal remedies against the Contractor. All insurance policies must be open to inspection by the State, and copies of policies must be submitted to the State's Authorized Representative upon written request.
- 1.4.1 Because the Contractor's reseller(s) are independently owned and operated, and maintain their own insurance, the Contractor's reseller's insurance coverage must be evidenced by its own Certificate of Insurance. The Contractor's reseller's Certificate of Insurance must meet all the insurance requirements and limits set forth in the Contract.
- 1.4.2 The Contractor shall collect, review, approve, and maintain the applicable Certificates of Insurance, including but not limited to General Liability, Auto Liability, Umbrella, Workers' Compensation, and Garagekeepers or Property of Others, for all Contractor's resellers that will be providing goods or services under this contract. The Contractor acknowledges compliance with this provision. The Contractor must provide copies of the dealers' insurance documentation to the State upon request.
- 1.4.3 If a claim is made against a Contractor's reseller, and the Contractor's reseller's insurance coverage did or does not cover the claim, the Contractor is responsible for the claim because the contract is with the Contractor. The Contractor must pay any uninsured claims out-of-pocket. The State may enforce the indemnity clause in the contract.

2. Notice to Insurer.

- 2.1 The Contractor's insurance company(ies) waives its right to assert the immunity of the State as a defense to any claims made under said insurance.
- 2.2 Insurance certificate holder should be addressed as follows:

- a. State of Minnesota
50 Sherburne Avenue, Room 112
St. Paul, MN 55155

3. Additional Insurance Conditions. The following apply to the Contractor, or the Contractor's subcontractor:

- 3.1 Contractor's policy(ies) shall be primary insurance to any other valid and collectible insurance available to the State with respect to any claim arising out of Contractor's performance under this Contract.

- 3.2 If Contractor receives a cancellation notice from an insurance carrier affording coverage herein, Contractor agrees to notify the State within five (5) business days with a copy of the cancellation notice, unless Contractor's policy(ies) contain a provision that coverage afforded under the policy(ies) will not be cancelled without at least thirty (30) days advance written notice to the State;
- 3.3 Contractor is responsible for payment of Contract related insurance premiums and deductibles;
- 3.4 If Contractor is self-insured, a Certificate of Self-Insurance must be attached;
- 3.5 Contractor's policy(ies) shall include legal defense fees in addition to its policy limits with the exception of professional liability.
- 3.6 Contractor's insurance companies must either (1) have an AM Best rating of A- (minus) and a Financial Size Category of VII or better, and be authorized to do business in the State of Minnesota or (2) be domiciled in the State of Minnesota and have a Certificate of Authority/Compliance from the Minnesota Department of Commerce if they are not rated by AM Best.
- 3.7 An Umbrella or Excess Liability insurance policy may be used to supplement the Contractor's policy limits to satisfy the full policy limits required by the Contract.

4. Coverages. Contractor is required to maintain and furnish satisfactory evidence of the following insurance policies:

- 4.1 **Commercial General Liability Insurance.** Contractor is required to maintain insurance protecting it from claims for damages for bodily injury, including sickness or disease, death, and for care and loss of services as well as from claims for property damage, including loss of use which may arise from operations under the Contract whether the operations are by the Contractor or by a subcontractor or by anyone directly or indirectly employed by the Contractor under the contract. Insurance minimum limits are as follows:

\$2,000,000 – per occurrence

\$2,000,000 – annual aggregate

\$2,000,000 – annual aggregate – applying to Products/Completed Operations

The following coverages shall be included:

- Premises and Operations Bodily Injury and Property Damage
- Personal and Advertising Injury
- Blanket Contractual Liability
- Products and Completed Operations Liability
- Other; if applicable, please list _____
- **State of Minnesota named as an Additional Insured**, to the extent permitted by law

Evidence of Subcontractor insurance shall be filed with the Contractor.

- 4.2 **Workers' Compensation Insurance.** Statutory Compensation Coverage. Except as provided below, Contractor must provide Workers' Compensation insurance for all its employees and, in case any work is subcontracted, Contractor will require the subcontractor to provide Workers' Compensation insurance in accordance with the statutory requirements of the State, including Coverage B, Employer's Liability. Insurance **minimum** limits are as follows:

\$100,000 – Bodily Injury by Disease per employee

\$500,000 – Bodily Injury by Disease aggregate

\$100,000 – Bodily Injury by Accident

If Minn. Stat. § 176.041 exempts Contractor from Workers' Compensation insurance or if the Contractor has no employees in the State, Contractor must provide a written statement, signed by an authorized representative, indicating the qualifying exemption that excludes Contractor from the Minnesota Workers' Compensation requirements.

If during the course of the contract the Contractor becomes eligible for Workers' Compensation, the Contractor must comply with the Workers' Compensation Insurance requirements herein and provide the State with a certificate of insurance.

4.3 Professional Liability, Errors, and Omissions. This policy will provide coverage for all claims the contractor may become legally obligated to pay resulting from any actual or alleged negligent act, error, or omission related to Contractor's professional services required under the contract. Insurance **minimum** limits are as follows:

\$2,000,000 - per claim or event

\$2,000,000 - annual aggregate

Any deductible will be the sole responsibility of the Contractor and may not exceed \$50,000 without the written approval of the State. If the Contractor desires authority from the State to have a deductible in a higher amount, the Contractor shall so request in writing, specifying the amount of the desired deductible and providing financial documentation by submitting the most current audited financial statements so that the State can ascertain the ability of the Contractor to cover the deductible from its own resources.

The retroactive or prior acts date of such coverage shall not be after the effective date of this Contract and Contractor shall maintain such insurance for a period of at least three (3) years, following completion of the work. If such insurance is discontinued, extended reporting period coverage must be obtained by Contractor to fulfill this requirement.

Exhibit C: Specifications, Duties, and Scope of Work

The following documents are attached and incorporated into the Contract:

RapidSOS ALI 911 Response

Exhibit D: Pricing

1. Contract Pricing.

1.1 In General. Prices listed take into consideration all inherent costs of providing the requested goods and services. The Contractor agrees to pay any and all fees, including, but not limited to: duties, custom fees, permits, brokerage fees, licenses and registrations, government taxes, overhead, profit, parking permits, proper disposal of materials, insurance payments. The State will not pay any additional charges beyond the price(s) listed, unless otherwise provided for by law or expressly allowed by the Contract. Prices listed within Exhibit D are maximum prices. These maximum prices shall remain firm for the initial term of the Contract. The Price List may not include any additional terms or conditions. A unit price and a total for the quantity must be stated for each item quoted. Prices must be quoted in United States currency. Any increase to Contract pricing requires a duly executed amendment to this Contract. Contractor may provide lower pricing at its discretion without requiring a duly executed amendment to the Contract.

1.2 The product purchase price from the supplier must be verifiable with a quote, billing statement, or invoice upon request from the State or Ordering Entity.

2. Price Schedule(s).

The following price schedule(s) are hereby attached and incorporated into this Exhibit D as follows:

2.1 Exhibit D Price Schedule

Exhibit E

The following documents are attached and incorporated into the Contract:

RapidSOS EULA

Executive Summary

RapidSOS appreciates this opportunity to respond to this RFP on such an important topic. Our company's origins go back to Minnesota and we are grateful for the collaboration of 85 Emergency Communications Centers (ECCs) in Minnesota in building the RapidSOS platform over the past decade. Today 83% of Minnesota's primary and secondary ECCs access data from RapidSOS, with the majority using RapidSOS Portal every day to access critical incident data. A further 308 agencies use RapidSOS' responder application (IamResponding) for incident dispatch, coordination, location, and supplemental data.

With a majority of Minnesota ECCs already using RapidSOS Portal, the migration to Premium is simple for telecommunicators across the State. Additional tools, map layers, and functionality are provisioned within a familiar user interface, and quick training makes for an easy upgrade.

RapidSOS Premium provides the requested ALL mapping solution with device based hybrid (DBH) location and complements the mapping with data delivered from our extensive partner network (100+ partners and 540 million+ devices) with all of this shared with field responders (via SMS link or dedicated Responder app). The solution is built on RapidSOS Portal which is used by 5,152 agencies in the U.S. covering 93% of the U.S. population. The Premium package has been upgraded in hundreds of these agencies and procured at both the local, regional, and state-wide level.

We believe this proposal demonstrates our strong qualifications to serve the citizens of Minnesota, telecommunicators, and field responders, and we look forward to working with the ECN and State Procurement through the RFP process.

About RapidSOS	10 Years+ of Partnering with Public Safety: Collectively built the first emergency data platform linking 540M+ devices to 16,000+ agencies • Built over the past decade in partnership with thousands of ECCs and first responders • The largest emergency data provider to 9-1-1 and field responder agencies - linking 3.3 billion emergency data payloads into 16,000+ 9-1-1 and field responder agencies across 170M+ emergencies annually • RapidSOS' Advisory Board includes current or former leadership of NENA, APCO, IACP, IAFC, NG9-1-1 Institute, EENA, and the FCC • 97 RapidSOS employees (43% of the company) are dedicated to ECC field support, integration, and engagement • Funded by largest institutional investor base of any privately-held public safety company (investor base represents \$8.6 trillion); RapidSOS has raised \$300M+ in capital and deploys one of the largest R&D and operational budgets in the Public Safety space
---------------------------	--

RapidSOS Premium	Unified mapping application integrated into existing ECC software stack, SOPs, and responder applications with data from 540 million+ devices - Premium is a cloud-native feature/data rich version of RapidSOS Portal (used by 5,152 9-1-1 agencies across the US including 83% of MN's ECCs). - Location: RapidSOS serves as largest emergency location data provider in the US - Premium provides the most robust of these features (DBH location, app/sensor locations, ALI/carrier data) all integrated with local ESRI GIS data - Critical emergency data: Richest set of emergency data from health profiles, native language, telematics, railroads, hazmat, health sensors, alarms, gunshot/weapon detection, every major school safety platform, indoor maps, 3D maps → in total 3.3B emergency data payloads in '23 - Extensive set of tools: Text from 9-1-1, real-time text language translation, video streaming from caller, drone dispatch, 3D indoor maps, dispatch AEDs, see officer locations (beyond AVL - down to actual officer location) - Integrated with ECC & responder tech stack: Premium integrated with RapidSOS broader platform integrations with 4,400+ public safety software systems and variety of responder apps including RapidSOS' own mobile app (IamResponding) used today by 308 agencies across MN - Critical tool in mass incidents / network outages - Ability to view all incidents in a region in real-time to get immediate view of mass incidents; separate, redundant data pathway allows ECCs to see and text citizens reaching out to 9-1-1 even if 9-1-1 networks fail (see example from Nashville bombing) - Mission critical platform: SOC II Type 2, ISO 27001, 24/7 NOC/SOC; HIPAA / HITECH Type I; support 170M+ emergencies per year
Life-Saving Data	RapidSOS Premium Built on Largest Emergency Dataset in the US 540 million connected devices pass critical data in an emergency into RapidSOS Premium 100+ partners share critical data in an emergency with RapidSOS, from every major tech company to the largest telematics provider in the US, railroads, connected buildings, digital health devices, insurance companies, non-profits, multimedia, weapon/shot detection, etc. - Platform built with Red Cross, American Heart Association, and Direct Relief to allow any citizen to upload an emergency health profile for free: https://www.emergencyprofile.org/

NG9-1-1 Features	DBH location and network-based ANI/ALI displayed and plotted on an Esri map with correlating line connecting the two • Text from 9-1-1 • 9-1-1-initiated requests for location, photo and/or video from caller • Text language translation in over 300 languages and dialects
Training & Support	Extensive training and support operation: have trained 500k+ users to date • Public safety team with 800 years of combined experience • Dedicated Premium Concierge to provide post-implementation technical and training support on a bi-weekly (or weekly if necessary) meeting cadence for minimum of three months • State-specific roadshows, training events, webinars, train the trainers, public safety software vendor training, etc. (100+ conferences attended/yr) • Online learning program, field training, and support team • Email, phone, in-person support & integration for public safety

1. Work Plan

Mandatory Features

1. Solution must be delivered in a SaaS platform.

- a. SaaS to include:
 - i. No software installed on a local user computer,
 - ii. All updates to the procured solution at no cost to the State or end user,
 - iii. No requirement to provide a hosting environment to access the solution,
 - iv. Must be accessible via standard commercially available browsers.

M1. RapidSOS Work Plan Details:

- RapidSOS Premium does not require any software installation. RapidSOS Premium is accessed over the internet at www.rapidsosportal.com, and therefore does not require a hosting environment.
- Software updates are automatic and are provided at no cost to the State or end user. RapidSOS routinely executes major, minor, and patch release deployments on a weekly basis in the US Eastern time zone during business hours.
 - RapidSOS employs zero-downtime strategies in its deployment methodologies (full automation, active-passive DNS handoff to full-system alternative during deployment and verification) enabling RapidSOS to maintain high availability regardless of deployment activities.
 - No feature deployments are undertaken on weeks containing US federal holidays where regular staff vacations are anticipated in public safety entities. No

deployments are undertaken in the weeks immediately preceding July 4th and January 1st each year.

This ensures stability and hardening prior to the spikes of traffic that routinely occur during these two highest-volume 9-1-1 traffic events of the year.

- The one exception is for emergency hotfixes with arbitrary timing (if needed) to correct an active or impending incident. No deployment activity is ever permitted outside of scheduled deployment windows
- End users can check their current version of the software at any time by clicking on the Menu icon within RapidSOS Premium (e.g. v5.6.0-32 as seen below).

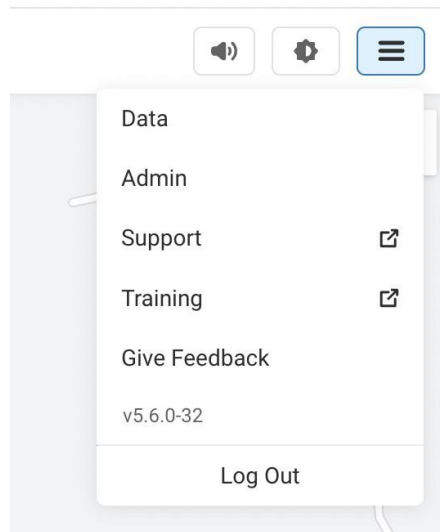


Figure 1: RapidSOS Premium Menu

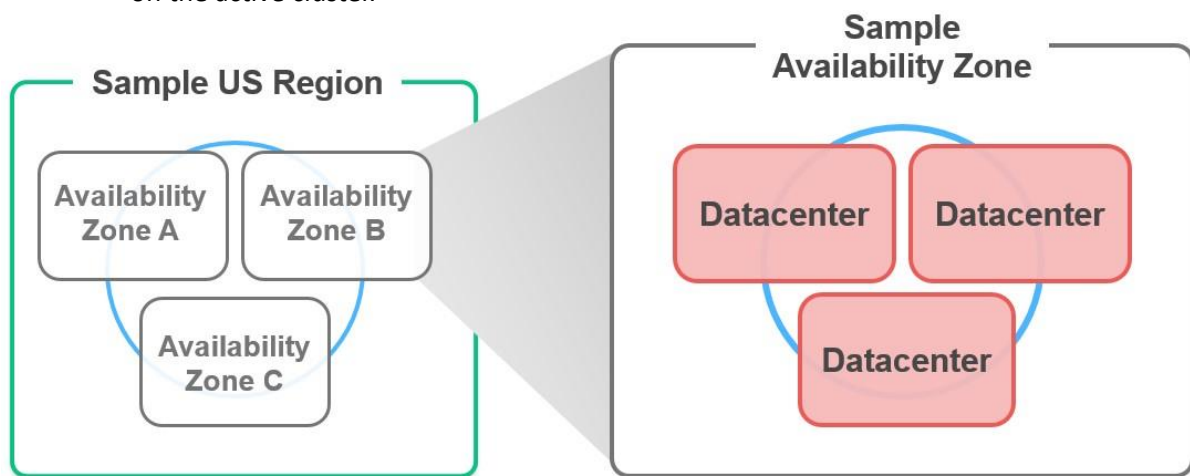
- RapidSOS Premium is web browser agnostic and can be supported by most widely available commercial web browsers.
- A benefit of this approach is that agencies with RapidSOS Premium automatically have access to the latest data sources and features inside RapidSOS (e.g. procuring RapidSOS Premium today also procures the benefits of the significant future R&D and data initiatives that RapidSOS is deploying).

M1. Major Tasks:

1. None. No additional tasks are required to meet the requirements.
2. Solution must be made available, and Data must be stored in a cloud-based location; access to the solution must be browser agnostic.
 - a. Please include, in your work plan, a diagram that illustrates:
 - i. How the end user connects to the application,
 - ii. Who stores the data/where it is stored, and
 - iii. What security measures are deployed protecting access to the data.

M2. RapidSOS Work Plan Details:

- RapidSOS uses Amazon Web Services (AWS) as a cloud-hosting provider. As the largest cloud service provider in the world, AWS is a key supplier to the proposed solution enabling the RapidSOS solutions with best in class IT infrastructure deployment. The quality of AWS datacenter infrastructure is unparalleled in terms of security, updates, scalability, and geographic redundancy. RapidSOS benefits from AWS' preexisting network operations and security operations that handle implementations of much larger scale in complexity making the day-to-day operation of the LIS and ADR very manageable. Application hosts in the cluster are split across at least three AWS availability zones in each region. Clusters are fully duplicated in AWS US-East and US-West regions in an active-passive configuration, setup for automatic failover at the DNS level in the event of trouble on the active cluster.

**Figure 2:** AWS Availability Zone data center example

- By default, RapidSOS' systems utilize an Elasticsearch stack deployed as a service per-cluster alongside services in that cluster in the same network with logging storage scoped per application service. As a result, the data stores and query interfaces inherit the same technical controls and permissions as the cluster they are deployed into, which RapidSOS manages via AWS standard IAM (Identity and Access Management) roles given only to authorized system administrator users per the policies of the RapidSOS Information Security Team. These policies (which are in scope of RapidSOS' ISO 27001:2013 framework and included in its SOC2 Type II certification, HIPAA / HITECH Type I), require segregation into completely separate AWS accounts for production vs non-production infrastructure, as well as transparent change-control for any IAMs permissions changes on production accounts.

RapidSOS AWS Storage Services

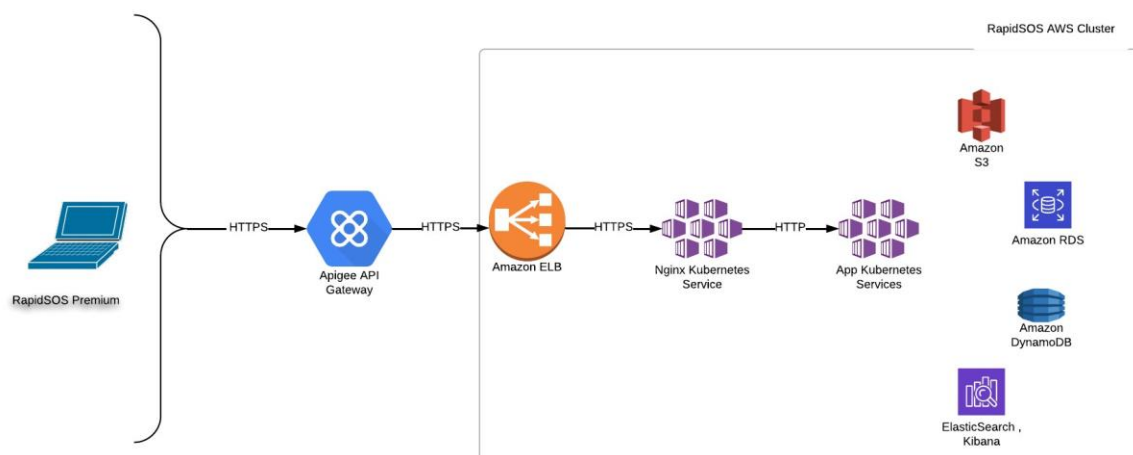


Figure 3: RapidSOS Cloud Storage

- AWS is ISO/IEC 27001:2013 certified providing security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how AWS perpetually manages security in a holistic, comprehensive manner. This widely-recognized international security standard specifies that AWS do the following:
 - Systematically evaluate its information security risks, taking into account the impact of threats and vulnerabilities;
 - Design and implement a comprehensive suite of information security controls and other forms of risk management to address customer and architecture security risks; and
 - Have an overarching management process to ensure that the information security controls meet its needs on an ongoing basis.
- In addition to ISO, AWS invests in myriad compliance regimes across its infrastructure and services. Table 1 below lists the AWS Assurance Programs.

Certifications/Attestations	Laws/Regulations/Privacy	Alignments/Frameworks
CMMC DoD SRG FedRAMP FIPS ISO 9001 ISO 27001 ISO 27018 PCI DSS Level 1 SEC Rule 17-a-4(f) SOC 1 SOC 2 SOC 3 HITRUST CSF	CLOUD Act FERPA HIPAA/HITECH IRS 1075 ITAR VPAT/Section 508	CJIS CSA FFIEC FISMA GxP (FDA CFR 21 Part 11) HITRUST MITA 3.0 MPAA NIST Uptime Institute Tiers

Table 1: AWS Security Assurance Programs

Infrastructure

Modern, Secure Microservices Architecture

RapidSOS worked with various providers to create a best-in-class modern cloud architecture – working with key component providers to virtualize even components previously only available on physical machines. This approach drives a number of benefits running a mission-critical data & communications platform:

- **Highly scalable** – RapidSOS infrastructure is auto-scaling, bringing on additional servers and resources automatically with demand.
- **Secure** – RapidSOS runs key components in siloed containers with highly restricted access.
- **Redundant** – RapidSOS manages its infrastructure across data centers in geographically diverse and redundant regions.
- **Auto-healing** – RapidSOS has multiple instances running at once, allowing RapidSOS to dynamically route traffic between different centers in the event of any failure event.
- **Contingency Planned** – RapidSOS is able to meet customer requirements for contingency plans including having their entire stack in a separate account that could be subsumed in the event of a going-concern event.

Data Encryption

RapidSOS has strict data encryption policies. Data is always moved via HTTPS on ingestion and HTTPS inside an IPsec site-to-site VPN interconnection to municipal networks. In NG9-1-1 networks, two-way TLS is used, with both client and server certificates issued by an authoritative public safety Certificate Authority.

Security

RapidSOS maintains a full information security management system (ISMS) and is ISO 27001/27002 ISMS and SOC II certified, which covers information security, human resources security, asset management and control, cryptography, etc.

RapidSOS maintains an ISMS Board that meets regularly to review the Company's security posture and conducts regular, formal risk assessments. Every employee goes through information security training and RapidSOS uses third parties to perform regular security audits.

M2. Major Tasks:

1. None. No additional tasks are required to meet the requirements.
3. Solution must allow for individual tenants of the solution to be configured for each end user agency.

M3. RapidSOS Work Plan Details:

- Each emergency communications center (ECC) within the State will have access to their own RapidSOS Premium instance. Individual ECCs will upload their GIS data to GeoComm's GIS Data Hub. This secure, browser-based application serves as the repository for ECCs to submit their data to be analyzed and then used in the creation of the hosted services for RapidSOS Premium. The initial and on-going annual GeoComm GIS data analysis, service creation, and data hosting are included in the standard annual Premium subscription fee.
- Each end user ECC will have the ability to configure RapidSOS Premium based on their own preferences. These configurations include options such as the data sources available to users, audible tones presented for calls/texts/alerts, ability to access specific tools such as drones, AED dispatch, etc., and color scheme for day and night modes.
- Individual features within RapidSOS Premium are configured by role-based access controls for each ECC account, which allow ECC administrators to enable permissions for specific features to relevant user groups.
- Through the admin panel, individual NG9-1-1 data sources may be turned on/off for each role.

M3. Major Tasks:

1. ECCs will complete data collection forms.
 2. RapidSOS will provision tenant access.
 3. Individual agencies will upload their GIS data to GeoComm's GIS Data Hub.
4. Configuration or user management must be done at the local tenant level, without requiring support by ECN or the State.

M4. RapidSOS Work Plan Details:

- Each ECC within the State will have access to their own RapidSOS Premium instance. These individual tenants will have the ability to add, delete, and edit users within their account. Each local tenant will also have the ability to create varying levels of access based on roles which allows them to configure what data sources are seen by each type of Role.
- Each ECC has access to 24/7/365 support coverage from RapidSOS through phone, email, ticket, and virtual meeting for any configuration or user management requests and/or questions.

M4. Major Tasks:

1. None. No additional tasks are required to meet the requirements.

5. Solution must provide a mapping function that displays Esri services (GIS base map data) with functionality where Individual end-user supplied GIS mapping services are added at the individual tenant (PSAP) level and only seen by those users.
 - a. The solution must enable the State to push GIS data to all tenants/users.
 - b. Please detail any additional mapping services that your solution uses.

M5. RapidSOS Work Plan Details:

- All users with access to RapidSOS Premium's Esri-based experience will have access to standard global Esri base map data including roads view and satellite view imagery.
- RapidSOS' system then allows for flexibility for additional basemaps and supplemental map layers for individual ECC configurations.
 - Each ECC's Esri-based web-hosted GIS service is configured to contain the desired GIS data set (whether statewide or ECC-specific). When each service is published, it is given a set of access keys, ensuring data is only accessed by the proper ECCs.
 - Once services are created for the necessary map services, RapidSOS performs ECC setup to match the proper services with the proper agencies.
 - For instance, the state may have a statewide basemap, containing all road centerlines, address points, and other relevant data for all jurisdictions within the State. Every participating ECC could be given access to that same service, so that when changes are made to that service, they are published everywhere simultaneously.
 - Services can also be created and enabled for individual ECCs, so that the unique needs of particular ECCs can be accommodated.
 - Each ECC is assigned a Premium Concierge to assist in configuring their specific supplemental map layers.
- The comprehensive GIS offering within RapidSOS Premium includes:
- **Initial and annual GIS analysis and report**
 - Certain data is needed for the RapidSOS Premium map to effectively validate locations and plot 9-1-1 calls through forward and reverse geocoding. As part of RapidSOS Premium, our partners at GeoComm – a Minnesota-based leader within the GIS industry – will conduct an analysis of the GIS data to ensure that critical data quality or completeness issues are identified upfront, so they can be rectified before going live with RapidSOS Premium. For multi-year contracts, subsequent annual checks are also included in the standard annual subscription fee to ensure data quality is maintained over time.
- **Basemap**
 - An ECC's configuration of RapidSOS Premium includes a basemap that leverages locally authoritative GIS data.
 - The basemap contains the kind of information that should be present at all times in your map and is useful to have for any and all calls. This includes Road Centerlines and Site/Structure Address Points, as a baseline, but can

include other supplemental information (i.e. city/state boundaries, parcels, bodies of water, etc.).

- The appearance of data will be optimized to suit the needs of different zoom levels. (For instance, address points will only appear once a user has zoomed in close enough to where they're looking at a focused area.)
- In addition to a locally authoritative basemap, RapidSOS Premium includes a global Roads View basemap and a global Aerial Imagery View, both provided by Esri. These basemaps are layered underneath the locally authoritative data and can be toggled on or off by users as needed.
- **Geocode Service**
 - A geocode service is used for determining addresses for calls appearing in RapidSOS Premium.
 - The geocode service will be configured to search Road Centerlines and Address points. This enables ECCs to leverage their locally authoritative data to determine the nearest address point for a caller, instead of relying on a global dataset that is outside of an ECC's control.
- **Supplemental map services**
 - ECCs can enhance their experience via rich and detailed GIS layers; however, an excess of data may have a performance impact on the mapping application. So the proposed RapidSOS Premium package includes two additional supplemental services. These layers, which unlike a basemap can be toggled on and off, work well for data that is not needed on every call and would otherwise clutter up a basemap. Examples include:
 - Responder boundaries
 - Recreational trails - hiking or walking trails
 - Utilities (e.g. water, sewer, storm water features)
- **Tooling to assist in ongoing data updates**
 - After the initial publishing of data as hosted services, the maintainer of the data – whether at the ECC level or the statewide level – can submit map updates via uploads to GeoComm GIS Data Hub.
 - Making corrections to the data itself is handled via the current SOP at the ECC or the State. However, the ECC or State can utilize the GeoComm GIS Data Hub admin capabilities provided with RapidSOS Premium to publish those updates to all users of the solution.



Figure 4: GIS data update process flow

- To accomplish this, the GIS contact at the relevant ECC can upload map data to GeoComm GIS Data Hub, using the same format, with the same layer names, and with the same attribute fields as the original data submission. From there, our partners at GeoComm perform data quality assurance checks and then republish.
- Once republished, all of the ECC's RapidSOS Premium users will have access to the updated data.

M5. Major Tasks:

1. Individual agencies will be given access to GeoComm's Online Data hub for GIS Data upload.
 - a. Mapping Requirements Document will be reviewed, completed and submitted during the onboarding process.
 - b. An end user account is created within GeoComm's GIS Data Hub, and credentials emailed to access the system.
 - c. For statewide services, a zipped Geodatabase of pre-aggregated dataset is uploaded to GeoComm's GIS Data Hub by the State GIS contact.
 - d. For ECC-specific services, a zipped Geodatabase is uploaded to GeoComm's GIS Data Hub by the GIS contact at the ECC.
 - e. The initial upload will undergo a quality check (QC). Once the upload passes QC, GeoComm configures the services for use in RapidSOS Premium, and the services are provided to RapidSOS to integrate into Premium.
 - f. After the initial publishing of your data, map updates can be submitted at intervals per the term of your subscription.
 - i. QC checks will be conducted on all maintenance submissions, and placed in queue for the next provisioning window. Once published, the updated GIS data will be pushed to all tenants / users via RapidSOS.
2. RapidSOS Implementation Team will configure each ECC's account with relevant endpoints for statewide or ECC-specific services.
3. ECC administrators have role-based access controls for GIS Services feature within RapidSOS Premium, and will grant permissions to desired user groups.

6. Solution must allow for a custom geocoder to be deployed and function in a hierarchical manner.

M6. RapidSOS Work Plan Details:

- As referenced above, a geocode service will be configured to search Road Centerlines and Address points.
- By default, RapidSOS Premium will use the geocode service powered by locally authoritative GIS.
- If that local geocoder fails to return a response, the application will fall back to using an Esri World Geocoder to ensure redundancy and availability of the application.

M6. Major Tasks:

1. Individual ECCs will upload their GIS data to GeoComm's Data Hub through the same process covered in Item 5.
 2. ECC administrators have role-based access controls for GIS Services feature within RapidSOS Premium, and will grant permissions to desired user groups.
7. Capability to display GeoComm indoor mapping products and a list of any other indoor mapping vendors the solution is currently interoperable with.
- a. Please detail any additional indoor mapping services that your solution uses.

M7. RapidSOS Work Plan Details:

- RapidSOS Premium supports fully embedded GeoComm indoor maps, meaning the indoor floorplans are overlaid atop the Esri-based map with location map markers placed atop the indoor floor plan to maximize situational awareness. A user can toggle on/off a map layer for GeoComm indoor maps. When turned on, as a user zooms in on the indoor map, the map becomes larger and the location map marker becomes very clear as to what room the call may be originating.



Figure 5: GeoComm Indoor Map embedded in Premium with officer location overlay

- Additionally, for indoor maps with multiple floors, a user may click on the indoor map to select other floor levels and display the map for each floor. This functionality can be especially useful when utilizing RapidSOS' Vertical Location Services powered by GeoComm.

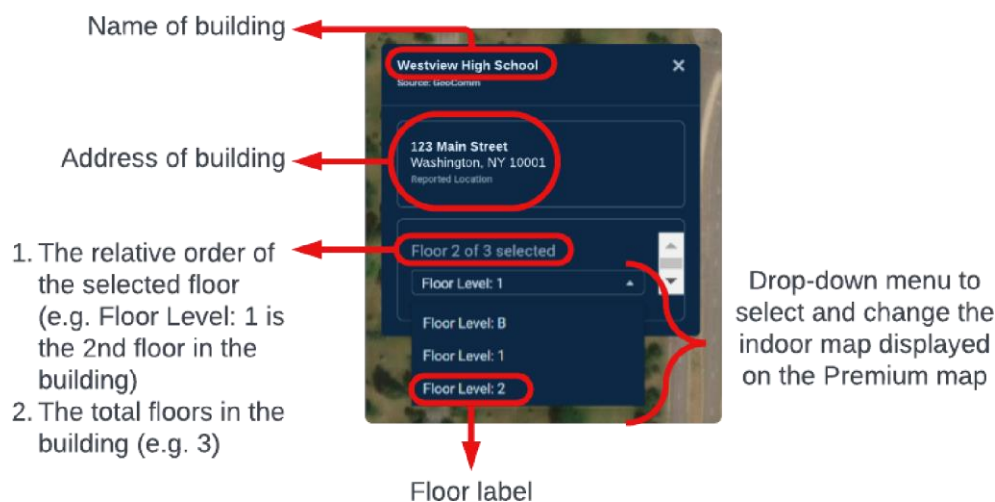


Figure 6: GeoComm Indoor Maps floor picker

- Vertical Location Services provides the telecommunicator with an estimated floor level based on a translation of the height above ellipsoid against the known elevation at the particular horizontal location.

< Back

GEOCOMM

Building detected at this location:

Showing results near 32.7030 , -117.1590 ↔ 33 feet ?

Building: Hilton Bayfront Hotel

Address: 1 Park Boulevard San Diego
Floor 24

Height: 330.57 feet above ground ↓ 16 feet ?

Floor: Caller is estimated to be on
Floor 24 (Likely range: Floor 23 - 25) ?

Accuracy: This is a low accuracy estimate ?

Feet per Story: 14 Update

Provide Feedback

ABOUT THIS SERVICE TERMS OF SERVICE GEOCOMM.COM

Figure 7: Vertical Location Services/Estimated Floor Level

- Telecommunicators can also access indoor floorplans made available via our partners at Critical Response Group Inc. (CRG) and 911inform. At the time of submission, RapidSOS has all three Collaborative Response Graphics® (CRGs) in Minnesota displaying within RapidSOS. Monthly updates ensure newly created CRGs are available in Premium.
- RapidSOS offers indoor floorplans, known as Collaborative Response Graphics, from CRG. CRG is the nation's leader in critical incident indoor mapping, having mapped over 15,000 sites across the country and adding hundreds every week. CRG maps schools, government buildings, airports, hospitals, corporate sites, and pre-planned events for security teams and public safety agencies. CRG visits every site to update and verify the accuracy of the indoor and outdoor mapping data.
- CRGs were transitioned from a mapping technique used in the U.S. military special operations community. CRGs are site-specific common operating pictures that enable better communication during an emergency. CRGs combine accurate floor plans, high resolution imagery, emergency response pre-planning, and gridded overlay into one map. CRG builds CRGs, distributes them to local, county, state, and federal public safety agencies through RapidSOS, and provides the necessary training to ensure full implementation.



Figure 8: Micro and Macro CRG examples

M7. Major Tasks:

- ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.
- Solution must obtain the Network location of 9-1-1 calls (ALI spill) data from either the 9-1-1 network directly or from the CHE (call handling equipment). Any other downstream sourcing of the data is not feasible as all 9-1-1 calls would not be displayed.
 - Please provide specifics as to how this data is obtained for the below:
 - diagram of data flow for the two different location variables (Network and DBH) to where that data is stored then accessed by end user,

- ii. Details on any needed installation of an appliances or hardware
- iii. Details on usage of any third-party providers/technologies should be listed.
- iv. Details on any requirements or end-user agreements specifically tied to accessing either source of location data.

M8. RapidSOS Work Plan Details:

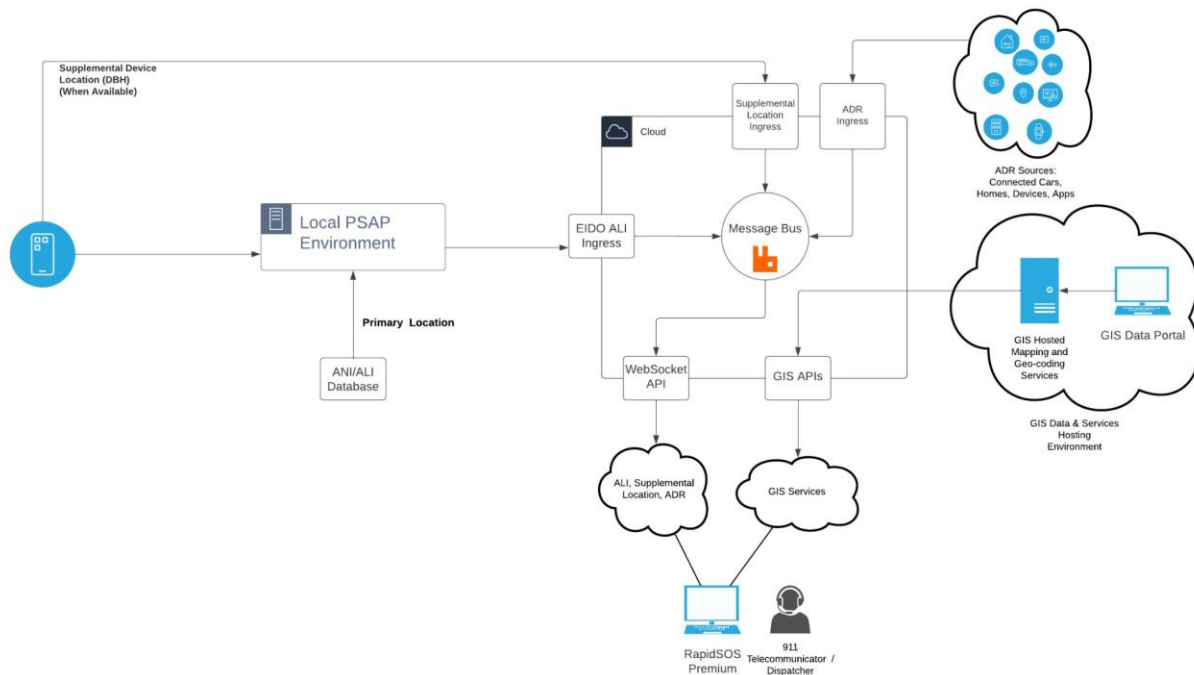


Figure 9: RapidSOS Premium Data flow Diagram

- For protection of Trade Secrets, RapidSOS will share additional details to this requirement in an interview or demonstration.
- RapidSOS provides services to intake the ANI/ALI from ECC systems and relay it for display on the RapidSOS Premium map. The ECC must provide internet access to utilize Premium.
- RapidSOS partners with GeoComm to bring an ECC's ANI/ALI feed into Premium which enables users to access 100% of 9-1-1 calls that come into a center. The ANI/ALI data also enables features like Call Taker Mode which automatically opens the specific incident being managed by a telecommunicator.
- ECCs that use RapidSOS Premium are required to sign one end-user license agreement for the application. A copy of this EULA may be found as an attachment to Section 5.

M8. Major Tasks:

- RapidSOS Implementation Managers will work closely with Local IT & appropriate ECC technical vendor resources to provision ANI/ALI data services to Premium.

9. Solution must allow for an over-the-top text-initiated location identification function.

M9. RapidSOS Work Plan Details:

- RapidSOS provides an over-the-top text initiated location.
- Each telecommunicator at an ECC will have the ability to send a text message with a link that will allow the caller to share their location.
- Location sharing begins when the caller agrees to share their location within the browser window that is opened by clicking the link from the text message.
- After the caller agrees to share, their device based location will populate on the RapidSOS Premium map and update location as the phone moves.
- The caller may disable location sharing by closing the browser. The telecommunicator can also disable location sharing by closing the call.

M9. Major Tasks:

1. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

10. Solution must allow for an over-the-top text-initiated live video feed sharing function.

M10. RapidSOS Work Plan Details:

- RapidSOS Premium provides over-the-top text initiated video.
- Each telecommunicator at an ECC will have the ability to send a text message with a link that will allow the caller to share their video.
- Video sharing begins when the caller authorizes to share video within the browser window that is opened by clicking the link from the text message.
- The video feed will display within the RapidSOS Premium window.
- Telecommunicators have the ability to turn on/off the remote participant's camera and audio for increased situational awareness.
- There are also role-based access to limit what a telecommunicator can see versus a supervisor including the ability to blur the video.
- Integrated chat and location is also available within the video experience.
- Text language translation is available in over 300 languages and dialects within the video experience.
- Video recording and archival is available to review the video for evidentiary analysis.
- The caller may disable video sharing by closing the browser. The telecommunicator can also disable location sharing by closing the call.

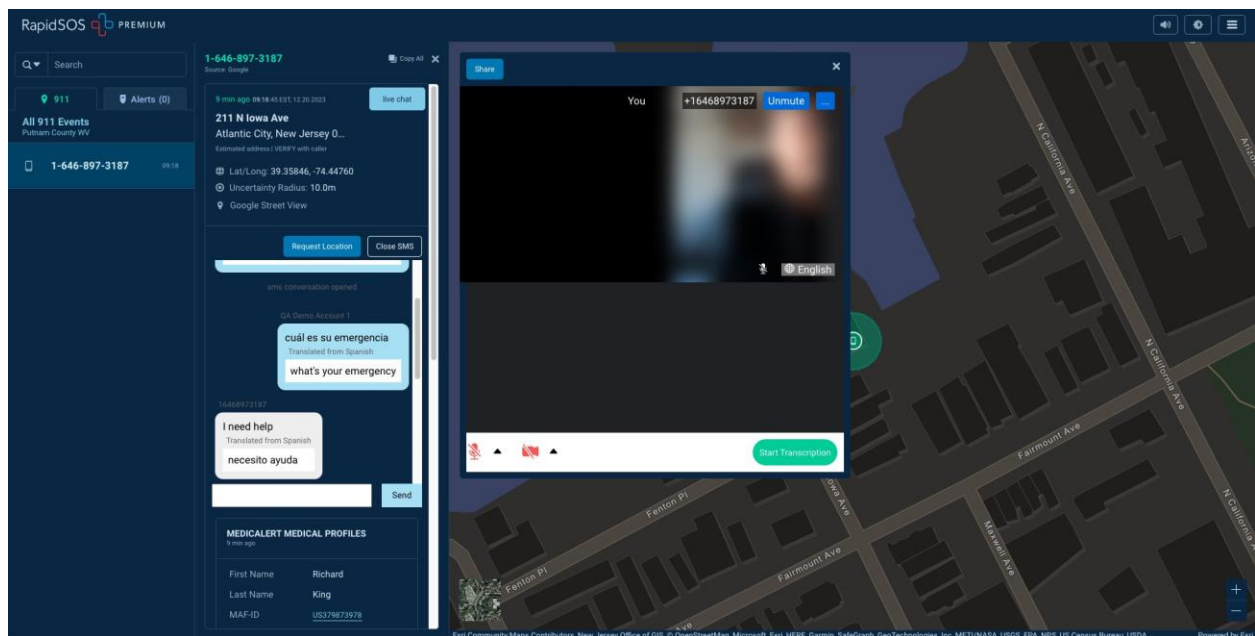


Figure 10: Live video and text translation inside RapidSOS Premium

M10. Major Tasks:

1. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

11. Solution must have map markup tools.

M11. RapidSOS Work Plan Details:

- RapidSOS Premium enables telecommunicators to mark up the map with points and polygons.

M11. Major Tasks:

1. ECC administrators will have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

12. Solution must come with the NENA EPRC PSAP registry to be enabled as a GIS basemap

- a. Please detail any additional cost in your Attachment C: Cost Detail for this functionality that may be required.

M12. RapidSOS Work Plan Details:

- Telecommunicators can load the NENA EPRC map layer inside RapidSOS Premium.
- No additional cost is required for enablement of this feature.

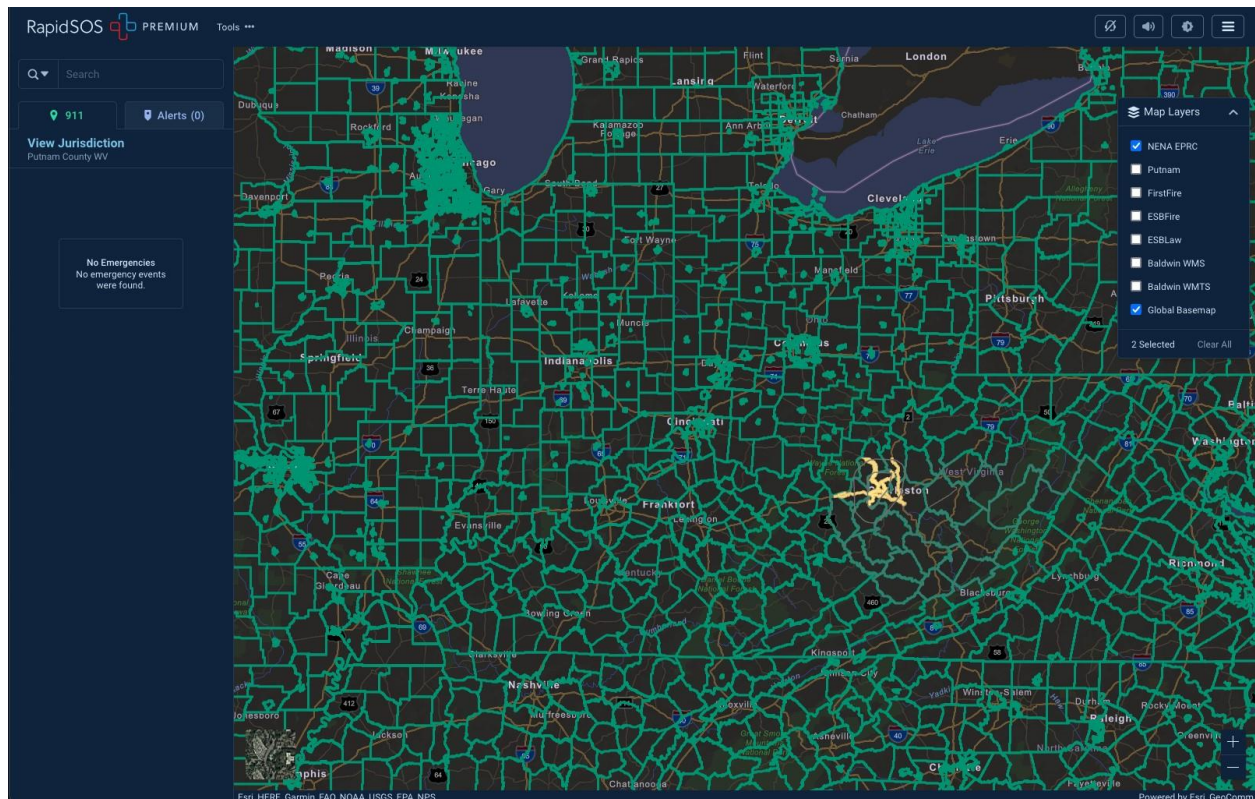


Figure 11: NENA EPRC inside RapidSOS Premium viewed in Night Mode

M12. Major Tasks:

1. ECC administrators will have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

13. Service must allow users to perform searches for addresses, points of interests, and place names, in addition to common geodetic formats such as latitude/longitude and What3Words.
 - a. Please detail all geodetic formats in use when conducting searches.

M13. RapidSOS Work Plan Details:

- RapidSOS Premium supports multiple types of searches, including addresses, cross streets, points of interest/place names, and latitude/longitude.
 - Telecommunicators can begin typing a search phrase and after the first few characters are entered, users will see a list of suggested results that they can select to find the relevant point on the map.
 - When searching for cross streets, users can indicate this type of entry by using the “@”, “&”, “\\”, or “|” symbol (eg. Central @ Walnut, Central & Walnut or Central \\ Walnut).
 - Searches will query an ECC’s locally authoritative GIS first. Esri search results are listed below the local information search results.

- Telecommunicators can select an option from the search results list to see that location on the map.
- RapidSOS Premium also supports searching by what3words locations.
 - Users can append a shortcode (///) to the beginning of their entry to find the relevant what3words location on the map.

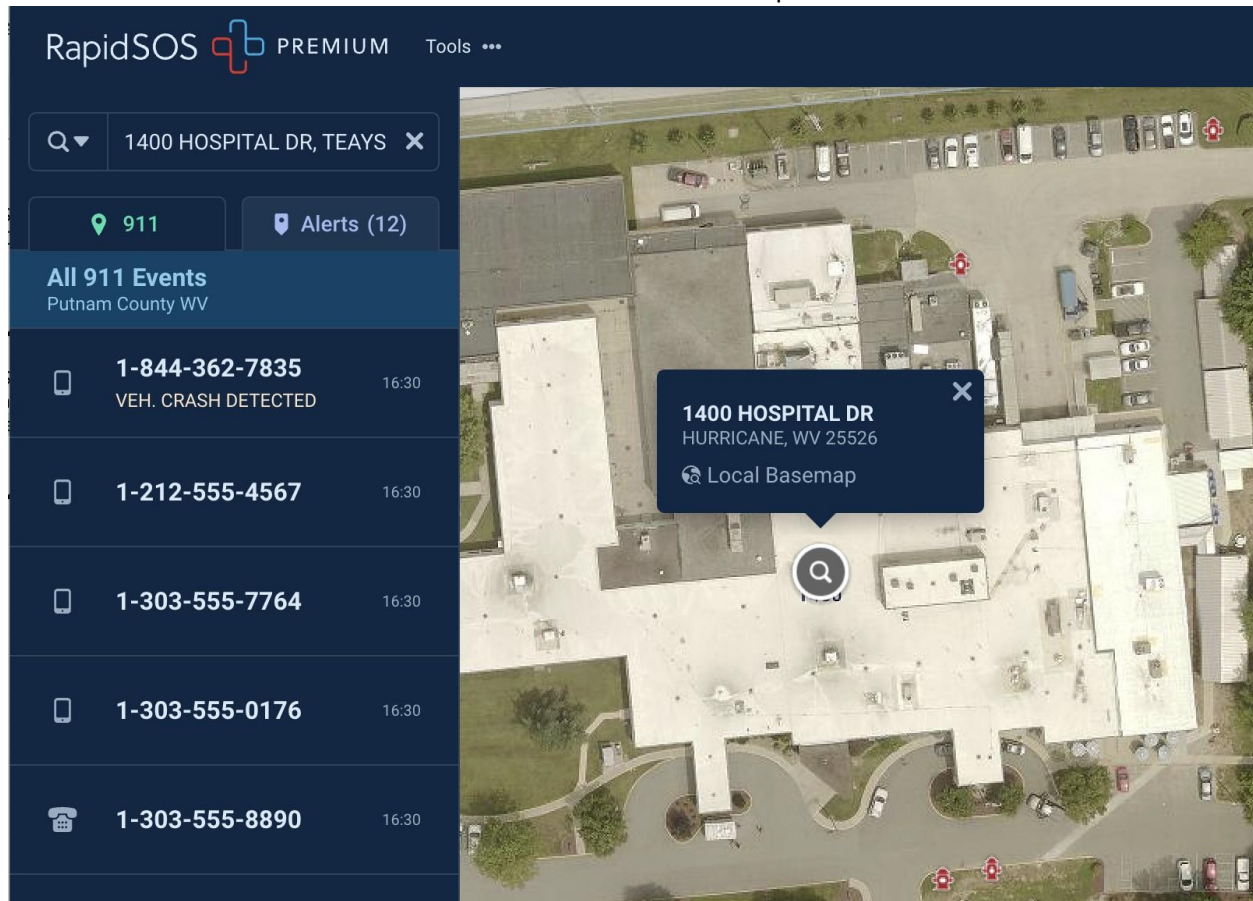


Figure 12: Screenshot of address search functionality in Premium

M13. Major Tasks:

1. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

Desired Features

1. A solution that provides the ability to display and respond to messages to specific users at peer agencies that include the fields needed for each agency to establish rules on how to handle the messages.

D1. RapidSOS Work Plan Details:

- RapidSOS “Agency Share and Chat” feature provides telecommunicators with the ability to send and receive messages to users at peer ECCs.

- Telecommunicators are presented with a list of peer ECCs with whom they can share/chat. The user selects the ECC(s) they wish to share/chat with and select the share button. The initiating ECC can add on other ECCs in the event they decide that they need to communicate with other ECCs. The added ECCs will see previous messages prior to when they joined the chat.
- Once the incoming share incident has been acknowledged, the chat window will automatically appear in the bottom of the event pane. Once populated, the chat window will provide the following information:
 - Header display of ECCs participating in the chat.
 - ECC name and ECC employee who is responding to the chat.
- The users can now actively chat in real-time. If there are multiple ECCs that have been sent an incident, then all ECCs will be in a group chat.
- Agency Share and Chat has role-based access control, so only users who are assigned this permission can chat with peer ECCs. (Note: Role-based access control is the mechanism to control which users receive messages, meaning the user sending a message doesn't have to take on additional overhead to determine which user may be online/best positioned to answer a given message.)

D1. Major Tasks:

1. Administrators at peer ECCs use RapidSOS Admin tools to establish the link between their ECCs.
2. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

2. [A solution that provides the ability to share an event derived from DBH location feeds with another user within or outside the user's tenant and include notes.](#)

D2. RapidSOS Work Plan Details:

- RapidSOS Premium provides "Agency Share and Chat" functionality. Agency Share and Chat allows ECCs to share an incident with selected peer ECCs. Peer ECCs are ones that are in a nearby jurisdiction (e.g., within the Minneapolis metro region) and can assist with mutual aid. (Peer ECC' boundaries are not required to be directly in contact with one another, but must be within a given range of distance apart. This means a metropolitan ECC, for instance, could pair with multiple ECCs in its outer suburbs.)
- With "Agency Share and Chat", users are able to share specific incident data to the peer ECCs. The user has the ability to share multiple incidents at the same time. After selecting an incident to share, the event pane will populate and the user will see an arrow next to the copy all function.
- Once the user clicks the arrow, they will be presented with a list of peer ECCs with whom they can share. The user will select the ECC/s they wish to share with and select the share button. The sharing ECC can add on other ECCs in the event they decide the incident needs to be shared to others. The added ECCs will see previous messages prior to when they joined the chat.

- Once the incoming share incident has been acknowledged, the chat window will automatically appear in the bottom of the event pane. Once populated, the chat window will provide the following information:
 - Header display of ECCs participating in the chat.
 - ECC name and ECC employee who is responding to the chat.
- The users can now actively chat in real-time on the incident being shared. If there are multiple ECCs that have been sent an incident, then all ECCs will be in a group chat.
- RapidSOS Premium users have the ability to see all incidents within their jurisdiction to improve situational awareness, so telecommunicators will be able to see the same information about a call as their peers within their own tenant.

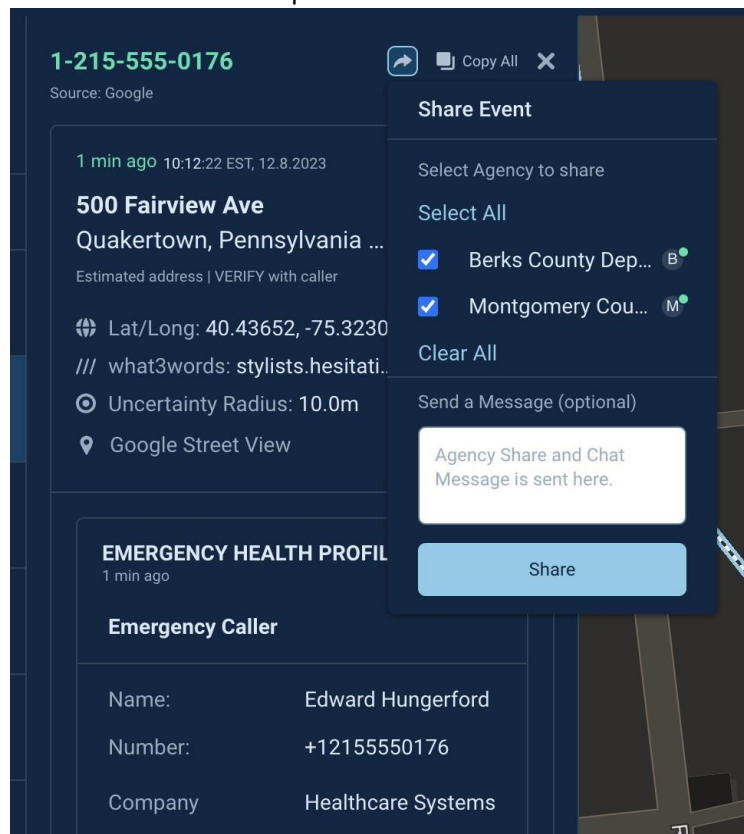


Figure 13: RapidSOS Agency Share and Chat feature

D2. Major Tasks:

1. Administrators at peer ECCs use RapidSOS Admin tools to establish the link between their ECCs.
2. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

3. Single sign-on with an end-user agencies active directory or other user management system.

D3. RapidSOS Work Plan Details:

- RapidSOS supports SSO functionality with partners to use their Identity Provider to log into RapidSOS.

D3. Major Tasks:

1. An IT contact at each ECC will input relevant information on the ECC's Identify Provider system, in order to activate the connection for each ECC.
4. [Interoperable with Rave Smart911.](#)

D4. RapidSOS Work Plan Details:

- RapidSOS has interoperability with Rave Smart911 today in that we flow DBH location, health/medical, telematics, and safety/security NG9-1-1 data to Smart911.
- Besides Rave Smart911, RapidSOS supports Apple Medical ID, Google Emergency Health Profile, EmergencyProfile.org Association (Red Cross, American Heart Association), MedicAlert Foundation, and a variety of other user profile/health databases.

D4. Major Tasks:

1. RapidSOS data is flowing to Rave Smart911 today and interfaces are available to deliver Rave Smart911 data to Premium. The State will need to ask Rave to activate the service where applicable.
5. [A platform to manage closed-circuit camera networks and capability to visualize them in the mapping application.](#)

D5. RapidSOS Work Plan Details:

- RapidSOS Premium supports inline video streaming. The sources of that data can vary:
 - Commercial video sources partner with RapidSOS to make their video feeds available to telecommunicators to provide situational awareness for nearby calls or incidents.
 - ECCs can also specify camera sources that are important to them (i.e. interstate traffic cameras) whose feeds can be ingested. Integration of such custom sources require an API from the originating provider indicating the location of cameras, links to streaming video feeds, and associated metadata that may be important to see context of the stream (i.e. name of the camera like "Front Entrance" or "Exit 415"). An example use case of this functionality is with the Virginia Department of Transportation cameras in Q1' 24.
- Publicly available and relevant local video cameras can be rendered if available as standard API services. If those solutions are hosted by the originating source (or their partner) and require additional fees to render in third-party applications, those fees would also be passed on to the end user or State.
- RapidSOS has signed partnerships with many of the largest consumer and commercial video security companies in the U.S. - collectively covering over ten million cameras across the country.

D5. Major Tasks:

1. ECC administrators have role-based access controls for this feature within RapidSOS Premium, and will grant permissions to desired user groups.

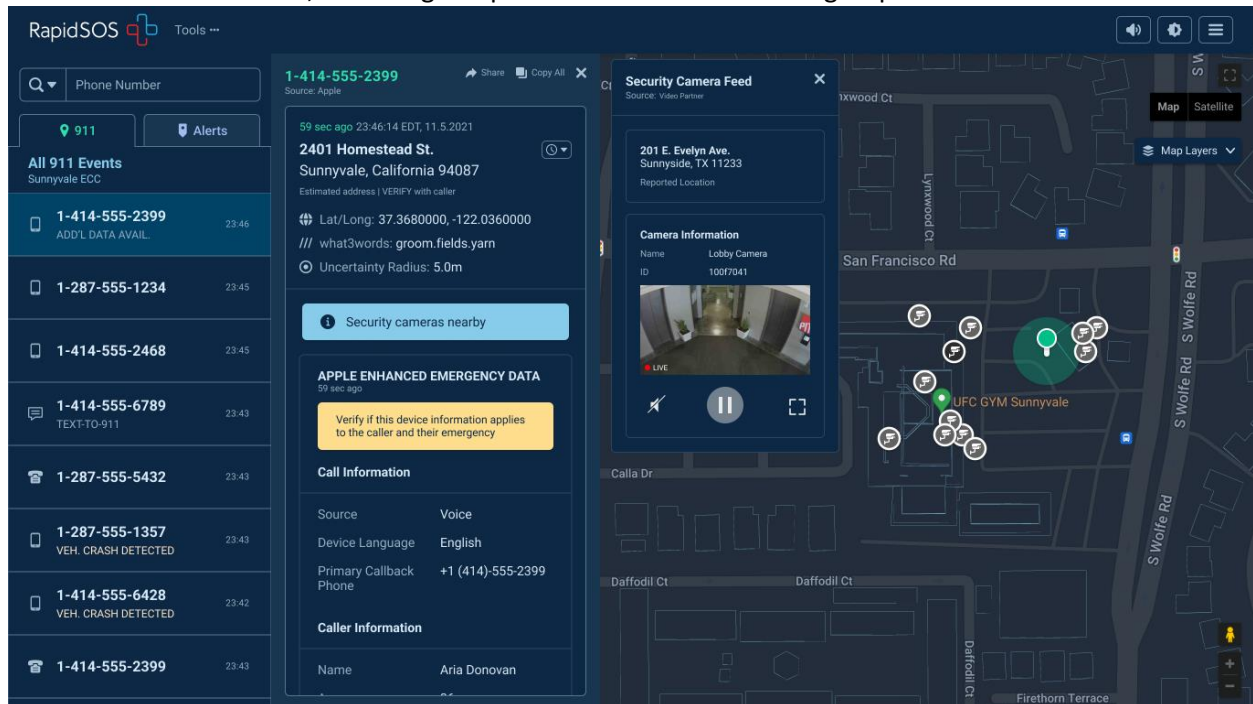


Figure 14: RapidSOS video display within Premium

6. Interoperable with EagleView aerial photography products, at no additional cost to the end-user or State.

D6. RapidSOS Work Plan Details:

- RapidSOS Premium supports displaying EagleView aerial photography products at no additional cost to the end-user or State.
- The orthogonal (top-down) aerial imagery is presented as a toggleable map layer in Premium.
- Today, RapidSOS Premium supports displaying orthogonal (top-down) aerial imagery provided through the following service types:
 - Web Map Service (WMS)
 - Web Map Tile Services (WMTS)
 - Esri Rest Map Service

D6. Major Tasks:

1. EagleView end points are provisioned for tenants with such assets.
2. ECC administrators have role-based access controls for GIS Services (including this feature) within RapidSOS Premium, and will grant permissions to desired user groups.



Figure 15: EagleView aerial imagery in Premium

7. 9-1-1 data analytics solution

D7. RapidSOS Work Plan Details:

- RapidSOS has developed custom 9-1-1 data analytics for customers across the 9-1-1 continuum, from originating location and data providers, to central station monitoring partners, and public safety.
- Current RapidSOS Premium customers are provided with 9-1-1 analytics reports showing an overview of ECC-wide activity, usage of specific features, user-level activity reporting, call data, etc. This report helps agencies understand their operation.

D7. Major Tasks:

1. None. No additional tasks are required to meet the requirement.

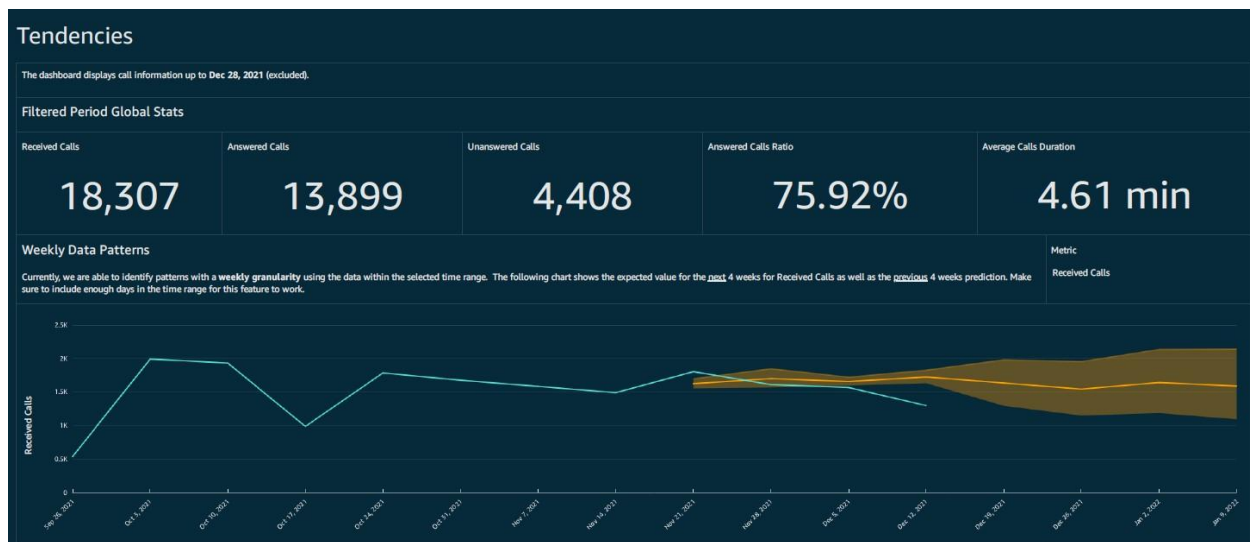


Figure 16: RapidSOS 9-1-1 Analytics - Custom Analytics Example

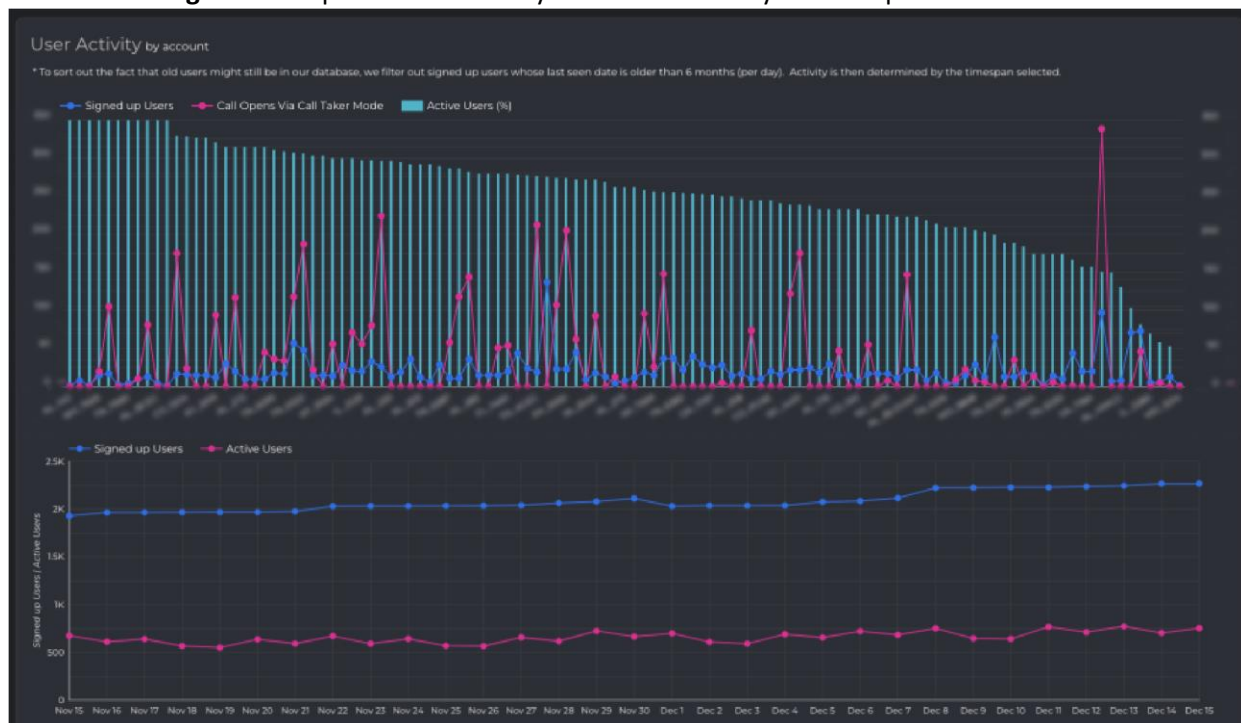


Figure 17: RapidSOS Premium Analytics - User Activity Report

- An additional data repository that is viewable through the mapping application but also aligns with the NENA definition:

An ADR (Additional Data Repository) is a data retrieval facility for Additional Data. The ADR dereferences a URI passed in a Call-Info header field or PIDF-LO <provided-by> and returns an Additional Data object block. An Identity-Searchable Additional Data Repository (IS-ADR) returns Additional Data associated with an identity.

D8. RapidSOS Work Plan Details:

- RapidSOS Premium offers additional data from a multitude of data providers inside the mapping application. The RapidSOS Additional Data Repository includes medical profiles, vehicle telematics, alarm data, and additional data associated with schools and buildings. Inside of RapidSOS Premium, an Identity-Searchable Additional Data Repository is offered when users type a telephone number URI into the search bar.

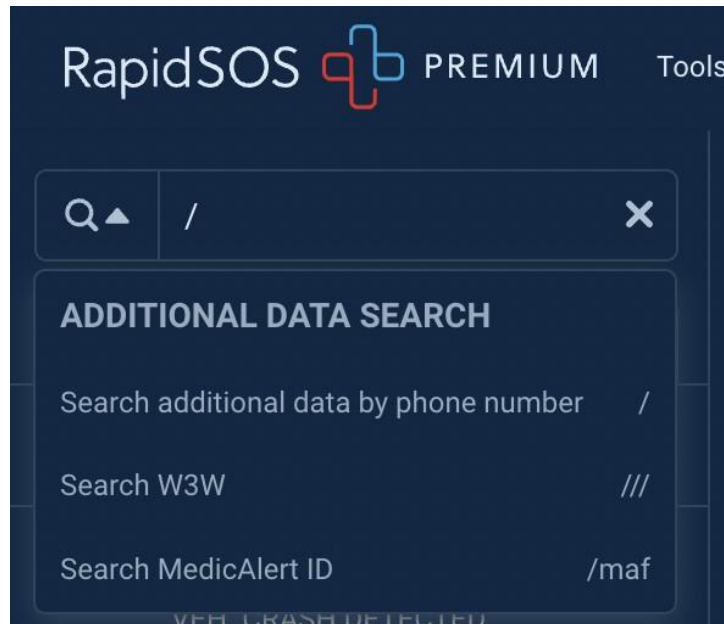


Figure 18: ADR identity search function within Premium

- In addition to additional data inside of RapidSOS Premium, RapidSOS makes the data available to other Public Safety Software Providers that are used by ECCs in the state. Both location data and additional data received by RapidSOS can be integrated into over 85 public safety software solutions from call handling and computer aided dispatch, to logging and mobile applications.
- RapidSOS provides a location interface to Public Safety Software Providers that responds to standard-compliant HELD requests that return the latest location in standard XML schemas per the NENA i3 architecture. It retrieves a Location Object using the HELD (HTTP-Enabled Location Delivery) Protocol according to IETF RFC 5985. Location objects are in the format of PIDF-LOs, Presence Information Data Format Location Objects (RFC 5139).
 - RapidSOS provides an additional data interface to Public Safety Software Providers that allows for querying additional data from various sources. Data from these sources is queried by phone number. It can also be queried by source-specific identifiers.

D8. Major Tasks:

1. None. No additional tasks are required to meet the requirements.

9. As needed on-site technical support throughout the contract.

D9. RapidSOS Work Plan Details:

- Each RapidSOS Premium ECC will be assigned a Technical Implementation Manager, Project Manager, and ECC Engagement Manager for dedicated support.
- RapidSOS provides on-site technical support, as needed, throughout the contract. RapidSOS has a team of experienced Technical Support Engineers that travel to ECCs as required.
- In addition to on-site support, RapidSOS Premium ECCs receive the below support services:
 - Technical Support via one number to call
 - A defined and documented escalation process for support cases
 - Return Materials (RMA) of any hardware provided by RapidSOS
- RapidSOS provides 24/7/365 support coverage through phone, email, ticket, and virtual meeting with a full multi-tiered team of Support Engineers, including after hours.
- Initial support response times average 6 minutes for all requests.
- RapidSOS has a full 24/7/365 NOC team that actively monitors our infrastructure, which allows us to proactively catch and immediately work to address any potential service outages or degradation.
- If necessary, service impacting events are broadcast to all users via a system status page and via in-product notifications.
- If any customer is experiencing a critical service outage, our NOC team can also be reached immediately through a dedicated emergency line.

D9. Major Tasks:

1. RapidSOS Implementation Manager will coordinate on-site technical support for Premium services during Implementation and RapidSOS Support will coordinate on-site support after go-live.

10. As needed on-site technical support for any implementation needs of hardware or solution configuration.

D10. RapidSOS Work Plan Details:

- RapidSOS provides on-site technical support for any implementation needs for both hardware and solution configuration. RapidSOS has a team of experienced implementation professionals that can travel to ECCs proactively or upon request.
- Each RapidSOS Premium ECC will be assigned a Technical Implementation Manager, Project Manager, and ECC Engagement Manager for dedicated support.
- In addition, RapidSOS provides each ECC with a dedicated Premium Concierge for three months on a bi-weekly (or weekly if necessary) virtual meeting cadence for structured post-implementation technical and training support. More details regarding the Premium Concierge within the “State of Alabama” example under “Similar Work Done” section below.

- RapidSOS provides any necessary hardware for an efficient and seamless implementation process.

D10. Major Tasks:

1. RapidSOS Implementation Manager will coordinate on-site technical support for Premium services during Implementation and RapidSOS Support will coordinate on-site support after go-live.

11. The solution, including third-party add-ons, delivered as a single contract that is executed by the State.

- a. Will you agree to provide template end user agreement for review and execution with individual PSAPs without changes from end user agreement as contracted?

D11. RapidSOS Work Plan Details:

- RapidSOS understands and agrees to provide the solution, including third-party add-ons, as a single contract executed by the State.
- RapidSOS agrees to provide a template end user license agreement for review and execution with individual ECCs without changes from the end user license agreement as contracted.

D11. Major Tasks:

1. None. No additional tasks are required to meet the requirements.

12. A mobile version/app where configuration and access of this mobile solution is managed at the desktop administrator level of individual tenants.

D12. RapidSOS Work Plan Details:

- RapidSOS Premium may be accessed via mobile phone and optimized for tablet use. The same configuration capabilities may be managed from the desktop administrator by individual tenants.
- RapidSOS also has a mobile application for field responders called IamResponding which provides 9-1-1 caller DBH location and additional data from RapidSOS Premium into the hands of responders in the field within their mobile devices.
- Administrators with access to the web application can configure and manage users on a granular level. Administrators can also restrict access to the mobile version from the web application if needed.
- Premium also allows an ECC to text a specific incident to a mobile version of Premium to any field responder.

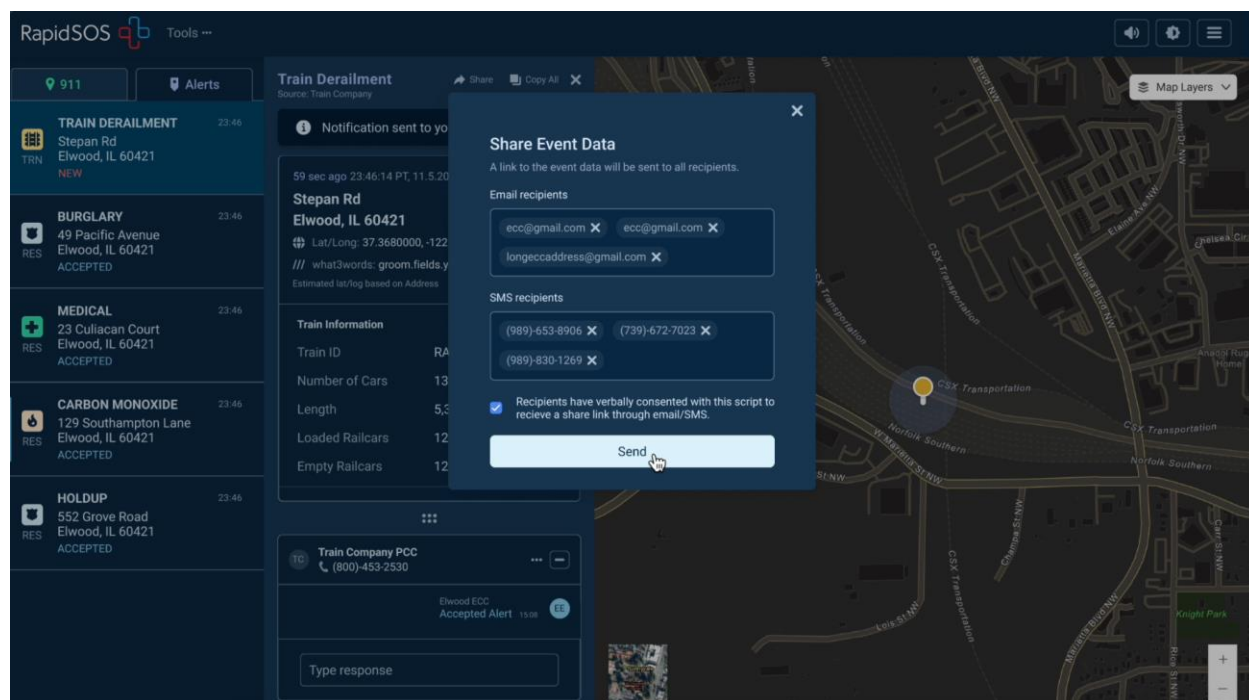


Figure 19: Share function for Train Derailment alert via text/email

IamResponding is an end-to-end emergency response and data platform and mobile application currently used by 10,000+ agencies and 470,000 field responders. 308 agencies in MN already use the service today. The service provides:

- Delivers time-saving alerts and critical incident data to emergency responders directly to their mobile devices.
- As a software-as-a-service system (mobile app, tablet app, and web browser application) which reduces emergency response times and enhances communications for all emergency responders including, but not limited to, members of fire departments, EMS agencies, law enforcement agencies, and regional response and rescue teams (such as Hazmat and Special Operations Teams).
- An efficient, reliable, easy to use and automated system through which emergency responders are alerted to emergency incidents and through which they provide their response status (responding or not responding, along with details of when and where) to their agency and/or response team, other members of that agency/team, regional response coordinators, and their dispatchers.
- Real-time location of field responders dispatched and responding to an incident is viewable both within IamResponding, as well as a map layer within Premium.
- Highly configurable granular user access and permissions configured via a web interface by agency system administrators.

lamResponding is a highly reliable and automated notification and emergency data system for providing emergency service providers with alerts of emergency incidents (inclusive via text message, email, push notifications to apps, telephone, voice, and fax). The redundant notifications originate both from CAD feeds (and/or self-dispatched notifications transmitted through users' lamResponding systems) and decoding pager tones and recording live dispatch audio, so that there is full redundancy if either source is experiencing transmission issues.

With lamResponding, emergency providers are immediately notified of emergency incidents, and emergency departments, agencies, teams and dispatchers know within seconds whether a full crew is en route, or whether a further dispatch needs to be issued for additional personnel. This results in a significant time savings compared to current dispatch processes and protocols.

lamResponding provides field responders with similar data that is currently available via RapidSOS Portal and Premium. This includes:

- Real-time DBH caller location
- Caller profile
- RapidSOS multitude of IoT sensor and other data feeds

lamResponding's customer support team brings decades of combined experience in the emergency services field, including members holding the positions of Fire Chief, Captain, Lieutenant, interior firefighters, exterior firefighters, and EMT's.

Experience and Current User Base

lamResponding is currently deployed and in use by more than 10,000 departments, agencies and specialty teams. Over 470,000 emergency responders currently rely on lamResponding every day.

lamResponding's Proven System and Network Reliability

The extensive network infrastructure of lamResponding is fully redundant, fault tolerant, geographically co-located (across multiple cloud hosting companies), and designed to provide 100% system up-time (99.99% uptime is assured, but lamResponding has delivered true 100% uptime for more than the past nine (9) consecutive years). There are no service or patch windows that cause any impact on the availability and functionality of the system, as lamResponding is able to seamlessly (and transparently to the user) migrate user sessions off of any servers that require any maintenance and onto other servers. There is 24x7x365 on and off-site internal and external monitoring, with 24x7x365 technical and network support. External server and network monitoring is provided through two (2) entirely separate and distinct monitoring systems, with each monitoring the servers and network performance from diverse geographical locations. There is

complete redundancy of all hardware incorporated within the network infrastructure, at every geographic location, with no single point of failure. The geographically co-located servers are fully active and fully synchronized, with no more than a four (4) second data gap between locations, and there is both automated and manual capability for full site-to-site failover within no more than five (5) seconds. lamResponding has proven itself through real-world use to be fully capable of delivering the most reliable web-based service in the emergency field response industry.

To date, lamResponding has successfully delivered more than 4 Billion alerts and messages to its users.

D11. Major Tasks:

1. RapidSOS will work with each subscribing agency to provision lamResponding services. To protect Trade Secrets, RapidSOS is unable to disclose additional details in the proposal, but will share additional details in an interview or demonstration.



Figure 20: lamResponding mobile app showing hydrants and location in school

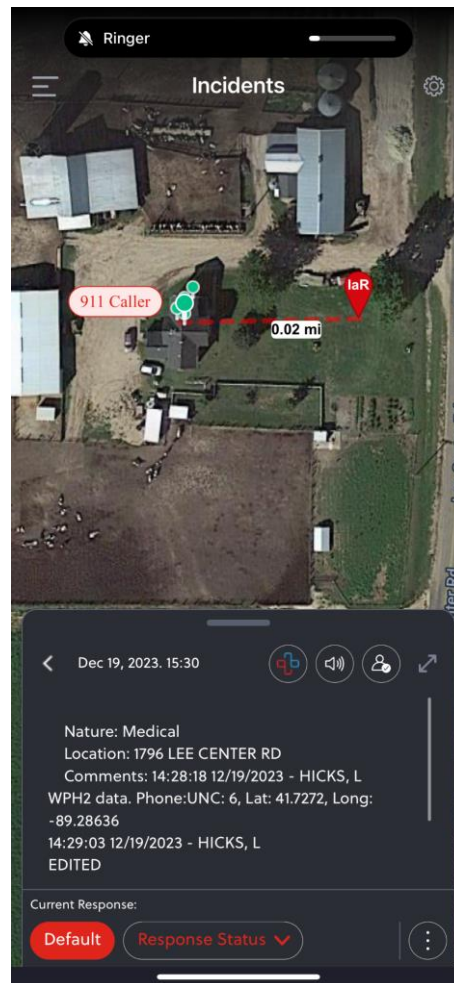


Figure 21: lamResponding mobile application displaying RapidSOS and CAD data

You Are Editing An Existing Member

Fields marked with * are mandatory

Mandatory Fields	
First Name	Gerald
Last Name	Smith
User Name	GERALDSMITH
Password	*****
Turn off system access	☐ ?

Figure 22: lamResponding Administrative Functions

2. Specifications

Attachment H: Requirements Matrix

REQ #		Y e s	N o	Exception
	Mandatory Features:			
1	Solution must be delivered in a SaaS platform (as described below):	X		
1a	No software installed on a local users computer	X		
1b	All updates to the procured solution at no cost to the State or end user	X		
1c	No requirement to provide a hosting environment or additional network connectivity to access the solution	X		
1d	Must be accessible via standard commercially available browsers.	X		
2	Solution must be made available and Data must be stored in a cloud-based location; access to the solution must be browser agnostic.	X		
2a	Please include in your work plan a diagram of how the user connects to the application, who stores the data, the security deployed protecting access to the data, and where the data is stored. Details must include any usage of a third party provider used for hosting or storage of the data.	X		
3	Solution must allow for individual tenants of the solution to be stood up for each PSAP.	X		
4	Configuration or user management must be done at the local tenant level (PSAP) without requiring support by ECN or the State.	X		
5	Solution must provide a mapping function that displays Esri services (GIS base map data) with functionality where Individual end-user supplied GIS mapping services are added at the individual tenant (PSAP) level and only seen by those users	X		
5a	The solution must enable the State to push GIS data to all tenants/users.	X		
5b	Please detail any additional mapping services that your solution uses.	X		

6	Solution must allow for a custom geocoder to be deployed and function in a hierarchical manner.	X		
7	Capability to display GeoComm indoor mapping products and a list of any other indoor mapping vendors the solution is currently interoperable with.	X		
8	Solution must obtain the Network location of 9-1-1 calls (ALI spill) data from either the 9-1-1 network directly or from the CHE (call handling equipment). <i>Any other downstream sourcing of the data is not feasible as all 9-1-1 calls would not be displayed.</i>	X		
8a	Please provide a diagram of data flow for the two different location variables (Network and DBH) to where that data is stored then accessed by end user. Please detail any third party providers in the diagram.	X		
8b	Please provide details on any needed installation of an appliances or hardware. Details on usage of any third-party providers/technologies should be listed.	X		
8c	Please provide details on any requirements or end-user agreements specifically tied to accessing either sources of location data.	X		
9	Solution must allow for an over-the-top text-initiated location identification function.	X		
10	Solution must allow for an over-the-top text-initiated live video feed sharing function.	X		
11	Solution must have map markup tools.	X		
12	Solution must come with the NENA EPRC PSAP registry to be enabled as a GIS basemap.	X		
13	Solution must allow users to perform searches for addresses, points of interests and place names in addition to all common geodetic formats such as latitude/longitude and What3Words.	X		

	Desired Features:	Y e s	N o	Exception
1	A solution that provides the ability to display and respond to messages to specific users at peer agencies that include the fields needed for each agency to establish rules on how to handle the messages.	X		
2	A solution that provides the ability to share an event derived from DBH location feeds with another user within or outside the users tenant and include notes.	X		
3	Single sign-on with a end-user agencies active directory or other user management system.	X		
4	Solution should be interoperable with Rave Smart911	X		
5	A platform to manage closed-circuit camera networks and capability to visualize them in the mapping application	X		In the development process. Production ready in Q1 '24 well ahead of any MN ECC deployment.
6	Interoperable with EagleView aerial photography products at no additional cost to the end-user or State.	X		
7	9-1-1 data analytics solution	X		
8	Additional data repository as defined in the NENA glossary	X		
	<i>An ADR (Additional Data Repository) is a data retrieval facility for Additional Data. The ADR dereferences a URI passed in a Call-Info header field or PIDF-LO <provided-by> and returns an Additional Data object block. An Identity-Searchable Additional Data Repository (IS-ADR) returns Additional Data associated with an identity.</i>	X		
9	Dedicated support staff for end users with the ability to go on-site quarterly.	X		
10	As needed on-site technical support for any implementation needs of hardware	X		

11	The solution provider must deliver the solution, even third-party add-ons, as a single contract that is executed by the State. All end-user agreements for solution functionality requirements or data to provide mandatory requirements must be eligible to be executed at the State/purchasing level.	X		
11a	Will you agree to provide template end user agreement for review and execution with individual PSAPs without changes from end user agreement as contracted?	X		
12	Solution must have a mobile version/app where configuration and access of this mobile solution is managed at the desktop administrator level of the tenant.	X		

Table 2: RFP Requirements Matrix (Attachment H)

3. Qualifications and Experience

Responder should provide an outline of background and experience with examples of similar work done by the Responder and a list of personnel who will conduct the project, detailing their training, and work experience.

Background and Experience

In partnership with public safety, RapidSOS has spent over a decade building the world's first intelligent safety and response platform. Today that platform is used by 16,000+ ECCs and field responder agencies to manage over 170 million emergencies annually with 3.3 billion emergency data payloads. ECCs covering 93% of the United States use RapidSOS to provide faster, more effective emergency response for their citizens.

Premium, RapidSOS' flagship experience, fuses tenets of product development across public safety and most major technology companies into a rich 9-1-1 experience that adds advanced tools and functionality in a user interface that most 9-1-1 telecommunicators are already using / used to:

- Accurate device based location updated in real-time + ALI network location for all call types (wireline, VoIP, and wireless)
- Connected to 540M+ devices which pass critical vehicle telematics, caller profile, health data, connected building information, gunshot detection
- Rich tools/functionality: launch drones, dispatch AEDs, see responder locations, etc.
- Video streaming, texting, language translation
- Interoperability with 5,000+ ECCs using RapidSOS Portal, tens of thousands of field responder agencies via IamResponding or Axon, and ultimately any field responder using RapidSOS' ability to text a mobile version of a specific incident in RapidSOS Premium to any field responder
- Integrated with state/local GIS data with full Esri experience & GeoComm data analysis

All of this built on a best-in-class, modern, scalable, secure cloud platform that has successfully supported 9-1-1 in managing over 500 million emergencies over the past five years.

RapidSOS Origins

RapidSOS was formed in 2012 by a team with Minnesota roots who had personal experiences needing help in emergencies. From those first experiences, RapidSOS began cold-calling 9-1-1 agencies across the United States to learn about the challenges those agencies faced. For the first three years, RapidSOS worked with over a hundred ECC/field responder agencies to study how data could be integrated across public safety software systems and standard operating procedures to drive a faster, more effective response. Ultimately, RapidSOS would study over 12 million 9-1-1 calls during this period.

RapidSOS was fortunate to collaborate with thousands of public safety officials and most major industry associations to develop its technology over this period, with past leadership of most major public safety associations joining RapidSOS' advisory board: the National Emergency Number Association (NENA), Association of Public-Safety Communications Officials (APCO), Industry Council for Emergency Response Technologies (iCERT), European Emergency Number Association (EENA), Next Generation 9-1-1 Institute (NG9-1-1 Institute), International Association of Chiefs of Police (IACP), International Association of Fire Chiefs (IAFC), and the Federal Communication Commission (FCC). This group of advisors would work closely with RapidSOS' ECC Advisory Board to drive the company's strategy and direction over the past decade.

This commitment to our mission has remained the guiding force across RapidSOS' organization. The RapidSOS team is made up of a rich mix of public safety veterans, technologists, experienced emergency response experts, and other business professionals. RapidSOS Portal and Premium are solely developed on U.S. soil with no off-shore influence. The RapidSOS technical team has experience at companies such as Accenture, Oracle, Athena, UBS, Comtech, Intrado, GeoComm, and Motorola Solutions amongst many others. RapidSOS' Public Safety team has over 800 cumulative years of public safety experience and a record of leadership in the 9-1-1 community, including two past NENA presidents.

Building the Largest Emergency Data Platform

One of the lessons learned through this research was the critical need for public safety to access critical information from the devices, sensors, and databases already deployed across citizen lives. With this knowledge, RapidSOS built a team dedicated to working with technology companies to connect their systems to 9-1-1 and first responders in an emergency. Today, RapidSOS is the largest provider of emergency data in the United States, connecting over 540 million+ devices to 9-1-1 and first responders in an emergency. Examples of this include:

- Real-time location updates
- User demographic and health profiles (big tech, non-profits, insurance companies, etc.)
- Vehicle telematics (tens of millions of vehicles linked through car, fleet, or mobile device)
- Connected buildings (fire alarms, security systems, video systems)
- Gunshot and weapon detection (acoustic and video)

- Multimedia (consumer devices, security systems, cloud camera systems, municipal camera systems, etc.)
- Digital health devices

Deploying, Integrating, Training and Supporting Public Safety

The largest lesson learned from RapidSOS' collaboration with public safety was the need to integrate into their existing technology systems, operational flows, and security protocols. RapidSOS worked closely with every major public safety software provider to integrate with their systems beginning in 2015. Today RapidSOS supports over 4,400+ public safety software integrations across its 16,000+ agencies.

In parallel, RapidSOS began partnering with national public safety training organizations to develop training, support, and integration capabilities. Since founding and in collaboration with IamResponding, RapidSOS has trained over 500,000 9-1-1 telecommunicators and field responders. Example activities in this area include:

- Train the trainer programs
- Attending/speaking at 100+ public safety conferences annually
- RapidSOS online learning program and portal
- In-app quick tips and features
- Field training and support
- State and regional roadshows

Funding a Commitment to Public Safety Partnership and R&D

RapidSOS has raised over \$300 million from some of the largest technology companies and investment firms in the world. Today, the company has over \$100 million in cash and no debt. RapidSOS' strong balance sheet enables one of the industry's largest commitments to research and development and public safety field support and training.

Similar Work Done

RapidSOS Premium adds additional functionality to RapidSOS Portal. One significant benefit is that most 9-1-1 telecommunicators are users of this platform (5,152 agencies covering 93% of the U.S. population). This existing deployed user base significantly accelerates RapidSOS' ability to implement and onboard users on RapidSOS Premium (an upgraded version of Portal). For example, significant time savings are found in the initial ECC configuration, since boundary files have already been reviewed and processed by RapidSOS' location solution providers. This results in a reduced implementation timeframe compared to other solutions in the market.

This extensive footprint also means that RapidSOS has experience implementing, training, and supporting everything from small rural agencies to the largest cities in the Americas (New York City, Los Angeles, Mexico City, Rio de Janeiro, etc.). For example, RapidSOS currently supports what we believe is the largest video into 9-1-1 program in the world with live 9-1-1 caller video streaming in Mexico City.



Figure 23: RapidSOS' COO, José Mejia, observing live 9-1-1 caller video streaming at Mexico City's C2 (police dispatch center)

As a data-driven company, RapidSOS has significant experience in creating valuable data insights to its commercial and public safety customers. Reporting on trends, correlating spikes in call volume, and platform usage are a few examples of similar work that RapidSOS supports its customers today.

State of Alabama - 9-1-1 Mapped ALI Solution

The Alabama 9-1-1 Board had a goal of providing a common operating picture across the state that allowed them to capitalize on the GIS development work that was in progress. As the GIS work was being completed, the Alabama 9-1-1 Board decided to run a parallel path to implement RapidSOS Premium to provide the common operating picture.

Implementing RapidSOS Premium enabled Alabama ECCs to capture the data from RapidSOS' NG9-1-1 data sources and make it more actionable by visualizing it within the Premium environment. The partner data helped to address industry trends and field responder requirements to share their location back to the ECC within Premium.

Tennessee Emergency Communications Districts - 9-1-1 Mapped ALI Solution

Despite a multi-year state contract for a different mapped 9-1-1 ALI solution, to date, 33 of the state's 100 emergency communications districts have decided to purchase RapidSOS Premium at their own expense. The decision by 33 ECCs to purchase RapidSOS Premium outside of the state contract is a testament to the value that RapidSOS can provide to emergency communications agencies. RapidSOS is a reliable, accurate, and redundant ALI solution that can help agencies save lives.

There were many reasons cited in procurement processes, including:

- Trust: ECCs expressed trust in RapidSOS as a company and its ability to deliver a reliable and accurate location solution.
- Redundancy: ECCs wanted to have a redundant location solution in place in case the NG9-1-1 solution failed.
- Relevance of the additional data: ECCs wanted access to the additional data that RapidSOS could provide, such as caller location history, health profiles, hazmat data, connected building data, and telematics data.
- Partnerships: ECCs were impressed with RapidSOS' partnerships with other emergency response organizations, such as the National Center for Missing & Exploited Children.

Expectations for a Statewide Project

The RapidSOS Premium implementation team works closely with the ECCs to prepare and develop an effective implementation roll-out. In the Alabama statewide implementation, there was an extensive outreach effort to engage all ECCs in the state. Weekly project update meetings are held to review the current focus, areas of concern, and other timely topics. Access to project tracking tools is provided to all stakeholders displaying project status information for each ECC. In addition to the weekly meeting, project updates are provided when appropriate via email and by phone.

As new ECC projects are identified, the RapidSOS Premium implementation team immediately engages with the stakeholders to kick off the project. Two meetings are then scheduled with each participating ECC. An initial kickoff meeting provides a complete overview of the project. This call is meant to cover onboarding needs, project scope and overall timeline. A second meeting is then scheduled to enable and test RapidSOS Premium services with the ECC. During the second meeting, the ECC is also introduced to their RapidSOS Premium Concierge.

As an important part of the RapidSOS Premium experience, RapidSOS provides the Premium Concierge as the direct point of contact. The Concierge is an experienced ECC Engagement Manager (EEM) that is uniquely focused on the Premium experience. The Concierge is available for three months post-implementation before transitioning to the permanent regional EEM for each ECC. During this period, ECCs will meet regularly with their Concierge to discuss any questions, suggestions, and concerns that may arise.

The Concierge meeting cadence is normally bi-weekly but will be set to meet the ECC's specific needs. Any discussion point may be addressed at any time, however, the RapidSOS Concierge will endeavor to cover the following key topics during meetings:

- GIS, Base Map and layers, GeoComm Data Hub
- User interface experience and satisfaction
- Call Taker mode
- Utilization data
- ALI data spill
- Standard operating procedures and Training
- RapidSOS Premium Admin, Roles, and Integration Management

Resumes of Project Team Members

See the attached Addendum document containing resumes (inclusive of training and work experience) for the following team members relevant to this proposal:

- Edward Parkinson
- Karin Marquez
- Jamison Peevyhouse
- Jennifer White
- Zachary LaValley
- Emily Ingram
- John Katt
- Chad Somodi
- Leslie Whitham
- Keith Vivieros
- Troy Cordle
- Ruslan Karimov
- Raymond Bailey

Executive Summary Information Table for Reference

About RapidSOS	10 Years+ of Partnering with Public Safety: Collectively built the first emergency data platform linking 540M+ devices to 16,000+ agencies • Built over the past decade in partnership with thousands of ECCs and first responders • The largest emergency data provider to 9-1-1 and field responder agencies - linking 3.3 billion emergency data payloads into 16,000+ 9-1-1 and field responder agencies across 170M+ emergencies annually • RapidSOS' Advisory Board includes current or former leadership of NENA, APCO, IACP, IAFC, NG9-1-1 Institute, EENA, and the FCC • 97 RapidSOS employees (43% of the company) are dedicated to ECC field support, integration, and engagement • Funded by largest institutional investor base of any privately-held public safety company (investor base represents \$8.6 trillion); RapidSOS
	has raised \$300M+ in capital and deploys one of the largest R&D and operational budgets in the Public Safety space

RapidSOS Premium	Unified mapping application integrated into existing ECC software stack, SOPs, and responder applications with data from 540 million+ devices - Premium is a cloud-native feature/data rich version of RapidSOS Portal (used by 5,152 9-1-1 agencies across the US including 83% of MN's ECCs). - Location: RapidSOS serves as largest emergency location data provider in the US - Premium provides the most robust of these features (DBH location, app/sensor locations, ALI/carrier data) all integrated with local ESRI GIS data - Critical emergency data: Richest set of emergency data from health profiles, native language, telematics, railroads, hazmat, health sensors, alarms, gunshot/weapon detection, every major school safety platform, indoor maps, 3D maps → in total 3.3B emergency data payloads in '23 - Extensive set of tools: Text from 9-1-1, real-time text language translation, video streaming from caller, drone dispatch, 3D indoor maps, dispatch AEDs, see officer locations (beyond AVL - down to actual officer location) - Integrated with ECC & responder tech stack: Premium integrated with RapidSOS broader platform integrations with 4,400+ public safety software systems and variety of responder apps including RapidSOS' own mobile app (IamResponding) used today by 308 agencies across MN - Critical tool in mass incidents / network outages - Ability to view all incidents in a region in real-time to get immediate view of mass incidents; separate, redundant data pathway allows ECCs to see and text citizens reaching out to 9-1-1 even if 9-1-1 networks fail (see example from Nashville bombing) - Mission critical platform: SOC II Type 2, ISO 27001, 24/7 NOC/SOC; HIPAA / HITECH Type I; support 170M+ emergencies per year
Life-Saving Data	RapidSOS Premium Built on Largest Emergency Dataset in the US 540 million connected devices pass critical data in an emergency into RapidSOS Premium 100+ partners share critical data in an emergency with RapidSOS, from every major tech company to the largest telematics provider in the US, railroads, connected buildings, digital health devices, insurance companies, non-profits, multimedia, weapon/shot detection, etc. - Platform built with Red Cross, American Heart Association, and Direct Relief to allow any citizen to upload an emergency health profile for free: https://www.emergencyprofile.org/
NG9-1-1 Features	DBH location and network-based ANI/ALI displayed and plotted on an Esri map with correlating line connecting the two

	• Text from 9-1-1 • 9-1-1-initiated requests for location, photo and/or video from caller • Text language translation in over 300 languages and dialects
Training & Support	Extensive training and support operation: have trained 500k+ users to date • Public safety team with 800 years of combined experience • Dedicated Premium Concierge to provide post-implementation technical and training support on a bi-weekly (or weekly if necessary) meeting cadence for minimum of three months • State-specific roadshows, training events, webinars, train the trainers, public safety software vendor training, etc. (100+ conferences attended/yr) • Online learning program, field training, and support team • Email, phone, in-person support & integration for public safety

Exhibit D – Price Schedule**9-1-1 Automatic Location Identification (ALI) Solution**

1. The discounted recurring price per license paid by the State shall be based upon the aggregate number of software licenses used by ECCs within the State. RapidSOS and the State shall mutually agree upon an accurate and timely method of measuring the number of licenses in use to determine the price per license, as well as a fair and reasonable billing schedule related to the contract Effective Date.

Software Product	Aggregate Number of Licenses In Use Within State	Annual Per License Recurring Fee
RapidSOS Premium Ready 3	1 – 25	\$3,591
RapidSOS Premium Ready 3	26 – 100	\$3,112
RapidSOS Premium Ready 3	101 – 200	\$2,633
RapidSOS Premium Ready 3	201 – 300	\$2,394
RapidSOS Premium Ready 3	301+	\$1,915

*Pricing includes up to 4 GIS map services.

2. Discounted non-recurring implementation costs per ECC paid by the State for initial program activation and configuration.

Implementation of Software	One-Time Fee per ECC
Implementation Services RapidSOS Premium Ready 3	\$750

3. **Optional** discounted professional and consulting services if necessary and requested by the State.

Professional and/or Consulting Services	Hourly Rate
Professional Services	\$200

4. **Optional** solution component that State may decide to purchase at a discount as an additional enhancement to the Premium Ready 3 software product.

Optional Solution Component	Annual Recurring License Fee per Field Agency
IamResponding mobile application for field responder agencies (fire, EMS, police, etc.)	\$600

Premium License Agreement

Effective Date: August 3, 2023

This EULA or Terms of Use ("Terms") govern the manner in which you will access the RapidSOS, Inc. ("RapidSOS", "we," or "us") Premium platform ("RapidSOS Premium") or otherwise receive one or more associated RapidSOS services ("RapidSOS Premium Service(s)").

Definitions

- **RapidSOS:** means RapidSOS, Inc., a provider of emergency communications services, located at 3 Park Avenue, 22nd Floor, New York, NY 10016, and its affiliates and subsidiaries.
- **Agency:** means a Public Safety Answering Point (PSAP) or Emergency Communications Center (ECC), as defined in the rules of the Federal Communications Commission (FCC), requesting access to RapidSOS Emergency Information.
- **RapidSOS Emergency Information:** means information received by RapidSOS from RapidSOS Emergency Information Providers and provided by RapidSOS to Agency, or exchanged via an authorized third-party integration, or provided directly by the Agency or an authorized third-party, including but not limited to supplemental 9-1-1 caller location data, profile data associated with a 9-1-1 caller, incident data received or provided via text message, video feeds, translation services, or other 9-1-1 incident data.
- **Credentials:** means unique electronic credentials that allow Agency to access RapidSOS Emergency Information.
- **RapidSOS Emergency Information Provider:** means any person that provides RapidSOS Emergency Information to RapidSOS, including via wire or radio communications, which may include without limitation manufacturers of smartphones or other connected devices, operating systems service providers, application service providers, monitoring companies, etc.

RapidSOS Emergency Information Terms of Use

Agency explicitly acknowledges that the RapidSOS Emergency Information is provided for informational purposes only and is supplemental to location and incident data provided from other sources and displayed in call handling and computer-aided dispatch systems, and that RapidSOS Emergency Information should not replace other emergency location information and should not be exclusively relied upon in an emergency scenario. RapidSOS Emergency Information will only be used by Agency to respond to 9-1-1 emergency events. Agency will not use the RapidSOS Emergency Information in any manner or for any purpose that violates any applicable local, state, national, or international law, any right of any person, or use the RapidSOS Emergency Information for any illegal, unauthorized or other improper purposes. Agency specifically authorizes RapidSOS, and each RapidSOS Emergency Information Provider, to provide the other emergency communications services contemplated herein to provision RapidSOS Emergency Information to Agency. RapidSOS shall be permitted to share RapidSOS Emergency Information with authorized third-parties for the purposes of delivering services as necessary for response to emergency events.

Agency acknowledges and agrees that RapidSOS may from time to time collect and analyze data arising from the use of the RapidSOS Emergency Information in order to facilitate the delivery of the RapidSOS Emergency Information, improve RapidSOS's delivery of the RapidSOS Emergency Information and Agency's experience, provide anonymized data to current and potential Emergency Information Providers, and improve or develop RapidSOS services. RapidSOS shall not share this data with any third person except as explained in this End User License Agreement, as authorized by Agency, and for the purposes of delivering the RapidSOS Emergency Information or to the extent required by a subpoena, court order, agency action, or any other legal or regulatory requirement.

Credentials to Access RapidSOS Emergency Information

Agency hereby requests a unique set of credentials assigned to Agency that will allow Agency to access RapidSOS Emergency Information. Agency acknowledges that Agency is responsible for proper safekeeping of those credentials, and will immediately notify RapidSOS electronically to support@rapidsos.com should these unique credentials ever get exposed to unauthorized personnel or otherwise compromised. For security reasons,

RapidSOS reserves the right to disable credentials and re-issue new credentials at their sole discretion. In such case, Agency or Agency vendor will be notified by RapidSOS.

RapidSOS Premium Services

As part of RapidSOS Premium, Agency may receive one or more additional RapidSOS Premium Services. Agency acknowledges and agrees that by receiving a RapidSOS Premium Service, it is bound by the applicable terms below.

Digital Alerts

For Agency's access to Digital Alerts, it is acknowledged and agreed:

- Agency is specifically requesting data to be presented through the Digital Alerts service and receipt of such data may require changes to your operational workflow when responding to an emergency. RapidSOS shall be held harmless for any liability arising from such use or failure to use.
- Agency acknowledges that RapidSOS is only transmitting the data rather than originating the data; therefore RapidSOS cannot guarantee the accuracy of data provided or originated by a third party and shall be held harmless for any liability arising from any use or reliance on such data.
- Agency acknowledges that RapidSOS will make reasonable efforts to digitally display requests for dispatch of emergency services and that a phone call request may not be placed.
- Agency has been trained on how to use and respond to the Digital Alerts product. This is not to be confused with other supplement alerts offerings available from RapidSOS, where a phone call remains the primary request for service.
- Agency acknowledges that RapidSOS does not warrant or represent that all digitally displayed requests through Digital Alerts shall be free of error. Your agency further acknowledges that an act, omission, or failure may occur that prevents notification of a request from being received by your agency. Where an error, act, omission, or failure occurs that prevents notification of a request from being received, RapidSOS shall not be held liable.

- Agency acknowledges that false alarms may occur and that RapidSOS makes no warranties or representations, express, implied, or otherwise, as to the validity, accuracy, completeness, or performance of a request for dispatch displayed through the Digital Alerts service. ALL DATA RELATING TO THE DIGITAL ALERTS SERVICE IS PROVIDED “AS IS.”
- Agency agrees to share certain data, including, but not limited to, the receipt of requests for dispatch of emergency services, and/or records of actions taken by your agency with RapidSOS and third-parties, such as alarm monitoring companies, in order to improve the product offering. RapidSOS may monitor and collect configuration, performance, usage, and consumption data relating to the use of RapidSOS services, and may monitor your agency’s use of the RapidSOS services, in each case: (a) to facilitate the delivery of the RapidSOS services, (b) to improve the RapidSOS services and provide anonymized analytics, and (c) to ensure compliance with the terms of this Agreement.
- You agree that RapidSOS may note that your agency is capable of receiving Digital Alerts and that RapidSOS may use the name of your agency on company materials indicating agencies that may receive Digital Alerts.

Modifications

RapidSOS reserves the right, at its discretion, to change this Agreement on a going-forward basis at any time. Modifications are effective upon publication. Continued use or acceptance of RapidSOS data following such modifications will be deemed your acceptance of the modified Agreement. Agency will ensure that its Users agree at all times to the most recent EULA provided by RapidSOS. Disputes arising under this Agreement will be resolved in accordance with the version of this Agreement that was in effect at the time the dispute arose.

Meeting Minutes: MESB PSAP Roundtable

Date & Time: Tuesday, July 9th, 2024 1000-1200

Location: Hennepin County Sheriff's Emergency Communications Facility

Host contact: Matthew Bozovsky

Committee Chair: Heidi Meyer

Attended by:

Hennepin County SO – Matt B, Nichole B; **Anoka Co ECC** – Heidi M, Melanie L, Alec G; **MESB** – Jake J; **U of M** – Joe M, Robin C; **St. Louis Park** – Eric L; **Ramsey Co ECC** – Erin Q, Tianna M; **Allina** – Candy C; **Scott Co** – Breanna G; **MCTC** - Carri S; **Mpls ECC** – Leticia C; **MAC** – Tom G, Matt, Lauren

Agenda Items:

1. Introductions
2. Additions, changes to the agenda
3. Training (new employee and continuing ed.)
 1. Current in-service opportunities
 - i. [St Louis Park / Hennepin County conducting Regional Response Exercise October 21st 1300-2130 \\$50/pp](#)
 - ii. [Ramsey Co ECC – APCO course / new communication supervisors – email if interested – approximately \\$400/pp for the 3-day course](#)
 - iii. [MAC – human trafficking course 10/22-10/24; NENA advanced Fire course 12/10-12/12](#)
 2. CTO training / Roundtable
 - i. [Plans in place for revitalized CTO Roundtable group – will need passionate, visionary to drive the movement of creating a space for CTOs to share ideas and network – discussion of the need for networking platform, Teams or Google -](#)
 3. General training questions, updates, etc.
 - i. [Discussion about \\$75k grant for resilience – Blue Ethos seems to be the best bet – would offer 4-hour classes for all metro area Public Safety TCs – schedule TBD](#)
4. Events and exercises (plans, meetings, 205's, impact on operations)
 1. [ComX – Camp Ripley 8/19-8/22](#)
 - i. [Discussion about local agency hosting a course for ComL certification](#)
5. PSAP technical updates and info (CAD, radio, phone, and other systems)
 1. [Allina – Centra Square update to version 23.1.3 – still working on CAD to CAD with St Croix Co](#)
 2. [St. Louis Park – Viper 7.1 is live – auto abandoned call back, possible use of denial of service filter for a large-scale event](#)
 3. [Ramsey Co – CAD to CAD with Washington Co went live](#)
 4. [Anoka Co – Prepared Assist – transcription/translation; successful use of Intrepid for Coon Rapids Carnival](#)
6. QA/QI – general updates, questions, etc.
 1. [Ramsey Co – Corti – testing calls / still a work in progress](#)
 2. [Anoka Co – will be having CTOs do QAs on their trainees](#)
7. PSAP operational updates and information (management, staffing, schedules, significant changes) – around-the-table updates from each agency
8. **Meeting calendar 2024**
 - October 8th, 2024 – **Ramsey Co ECC ** note change ****

**Metropolitan Emergency Services Board
9-1-1 Technical Operations Committee
9-1-1 GIS/Data Report
September 19, 2024 Meeting**

Importance of GIS for 9-1-1: PSAP managers are strongly encouraged to assist their GIS counterparts in helping key decisionmakers and county leadership understand the **vital role GIS has for current and future PSAP operations**. Geospatial datasets provide foundational data for PSAP CAD/mapping systems and NG9-1-1 core services, as well as many non-public safety use cases important to counties and cities.

1. **Monthly Regional NG9-1-1 Regional Data Maintenance & QA/QC Cadence:**
 - a. The MESB region maintains a **monthly cycle NG9-1-1 data provisioning and maintenance**. This includes county GIS dataset maintenance, regional GIS data aggregation and schema validation, regional validations for the NG9-1-1 use case, and ongoing GIS-derived MSAG maintenance.
 - b. A summary of the monthly **regional NG9-1-1 data cadence** is included at the end of this month's GIS/Data report.
2. **Regional 9-1-1 Data QA/QC:**
 - a. MESB continues to **analyze the region's NG9-1-1 data errors** that are identified monthly through MESB's internal validation tools, GeoComm's GIS Data Hub (GDH), and 1Spatial's platform.
 - b. MESB also validates each month's actual 9-1-1 call locations against regional GIS to identify missing or inaccurate GIS data.
 - c. When needed, MESB reaches out to county GIS contacts to make recommended data remediations. If it is determined that MSAG and/or ALI updates are needed, MESB will process the update requests on behalf of its PSAPs.
 - d. From the **August** NG9-1-1 validations and MESB's error analysis:
 - i. MESB sent 59 new referrals related to address validation to county GIS data producers for GIS data updates. (There were 51 additional GIS referrals still outstanding that were carried over from July).
 - ii. MESB made 16 referrals for GIS updates resulting from VoIP 9-1-1 call location validation.
 - iii. MESB also issued multiple ALI Telephone Number record change requests (TM CRs) for needed wireline location corrections.
 - e. In September, MESB has also been working with county GIS partners are some geometry finetuning based on validations from the 1Spatial platform.
 - f. The **September** full regional NG9-1-1 data validation run was conducted on **9/10/24**. The results are currently being analyzed and referred to county GIS partners.
3. **Metro Regional GIS-derived MSAG Maintenance:**
 - a. **GIS Drives MSAG Maintenance:** The monthly regional NG9-1-1 data provisioning/maintenance cadence is now the **primary method of maintaining the region's live MSAG**. Basically, GIS updates drive the MSAG updates. Each month, MESB performs a comparison between the current live MSAG and the MSAG derived from the current month's refreshed GIS data. MESB then reviews/vets any needed updates prior to submitting them to Intrado on behalf of its PSAPs.
 - b. **GIS MSAG Change Requests through 911NET:**
 - i. As mentioned above, monthly, MESB submits any MSAG Change Requests (CRs) needed to keep the metro region's live MSAG data in sync with its NG9-1-1 GIS data.
 - ii. PSAPs no longer must carry primary MSAG maintenance responsibility through submitting 911NET MSAG CRs.
 - iii. PSAPs have the discretion to continue to submit MSAG CRs based on information obtained from cities or other sources if they choose; but it is most important to share that information

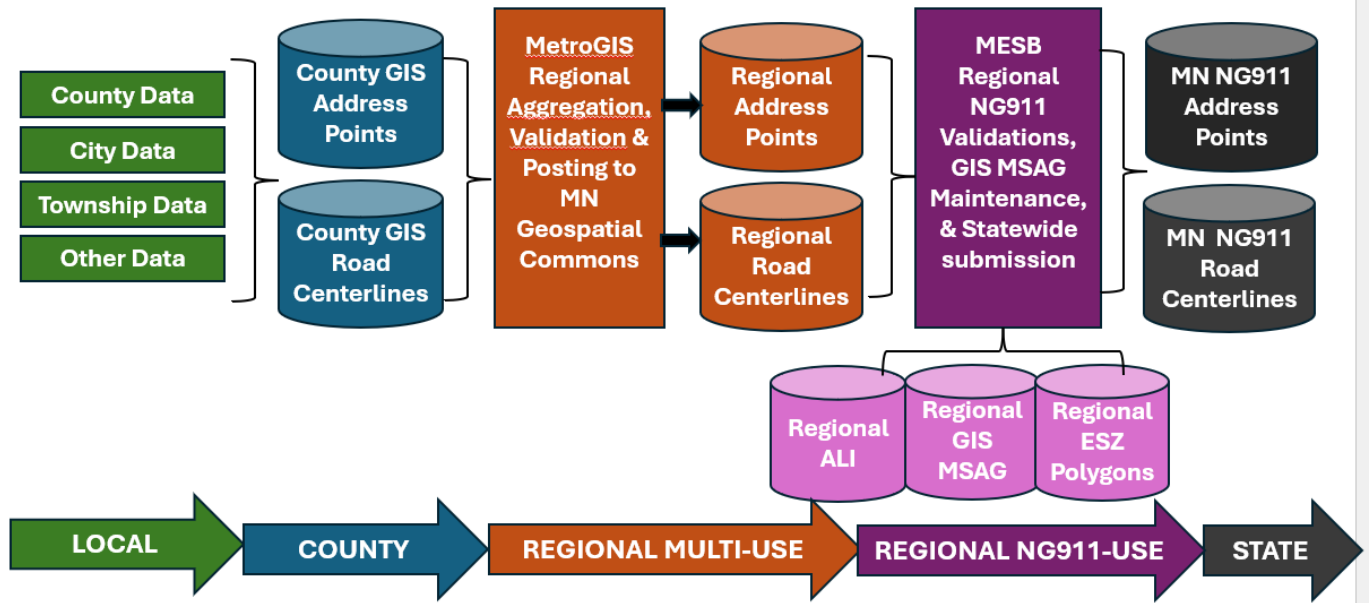
- with county GIS partners (if needed) to ensure the same information is flowing through the county's standard road and address processes.
- iv. To help ensure the live MSAG aligns with what is contained in the GIS data, MESB holds any PSAP submitted MSAG CRs until the updates appear in the county's GIS data. *Exception:* If substantial construction in the area becomes visible on aerial imagery and the GIS data is still missing, MSAG will process the CR temporarily and adjust the details, such as range values, later based on county GIS data.
 - c. **GIS-driven MSAG Maintenance Activity:** In August, MESB processed approximately 148 GIS-derived MSAG updates to keep the live MSAG in sync with authoritative GIS data.
4. **Interagency GIS Support Agreements:** Drafting is underway of the interagency GIS support agreement template to assist metro counties in **documenting the ongoing functions that county GIS data producers provide to metro PSAPs**. MESB will share the draft with PSAP managers as soon as it is available.
 5. **Wireless Call Routing:** Verizon continues to send through a large volume of cell sector routing requests to support their 5G build out throughout the metro region. MESB processes these routing requests on behalf of its PSAPs.
 6. **School Mapping Legislation:** Through various workgroups, MESB staff participated in the creation of feedback for the NG9-1-1 Committee about the recent school mapping legislation. Example GIS Workgroup feedback included:
 - a. **The business/operational needs of Minnesota schools and their safety officials, local public safety responders, and PSAPs should be well defined before GIS requirements are outlined.** Basically, the NG9-1-1 GIS workgroup feels that the purpose and use of the maps needs to be clearly articulated first.
 - b. **Maintenance is vital to the ongoing usefulness of any maps created under this legislation and needs to be addressed.**
 - c. **If interoperability and consistency with these maps is desired across the state, a common set of baseline requirements for map content, look and feel would be useful.**
 - d. School district and PSAP/region boundaries will likely not align, resulting in **cross-boundary coordination issues that may reinforce the need for data interoperability.**
 - e. **In most cases, the GIS work would likely not be done by existing county GIS staff.** Typically, county GIS staff members supporting the NG9-1-1 project would not be directly involved with indoor mapping, school safety, incident command, and local responders. In addition, based on previous experience with the NG9-1-1 GIS grants, the funding process is more straightforward using vendors than internal staff. GIS workgroup members also expressed concern about security and hosting responsibilities.
 - f. **Project management is anticipated to be a challenge in this effort.** Roles and responsibilities surrounding this will need to be **clearly defined and adequately staffed.**
 - g. Indoor maps have the greatest utility as **part of comprehensive school safety and response plans. Including site details/plans** (not just indoor aspects) is beneficial. The maps are best positioned as one tool in plans coordinated by schools, emergency managers, first responders, and PSAPs.
 - h. The digital maps should be **easily integrated into systems used by PSAPs and available in multiple formats to allow ease of use by those responding in the field.** Regardless of any mechanisms for electronic display of indoor maps, consider having vendors also make the maps **available in a printable file format** such as PDF.
 - i. Given the constraints of the legislation, SECB grant funding processes, and stakeholder needs, the NG9-1-1 Committee may want to recommend that the SECB **consider engaging a consultant with specific expertise to:**
 - 1) Create and guide a statewide vision/scope for the project;
 - 2) Engage a steering group of statewide stakeholders (including schools and responders) to define and document baseline needs and expected deliverables;
 - 3) Create a project framework (e.g., plan, schedule, roles, responsibilities, and management) that leverages successful experiences in other states but fits the MN-specific constraints;
 - 4) Define ways to avoid duplication of effort and create consistency;
 - 5) Support the regions in the tasks defined for them in the legislation.

7. **SECB NG9-1-1 GIS Workgroup:** The GIS Workgroup continues to meet monthly to discuss topics of interest to statewide GIS stakeholders:
 - a. **Best practice on Periodic NG9-1-1 GIS Data Resubmission:** This has been passed to the SECB NG9-1-1 Committee for consideration.
 - b. **Best practice on MSAG and ALI TN Change to Support NG9-1-1 Data Preparation:** This has been passed to the SECB NG9-1-1 Committee for consideration.
 - c. **Indoor Mapping of Schools:** The workgroup prepared feedback to the NG9-1-1 Committee on Minnesota's legislation allocating \$7 M for digital indoor mapping of schools.
 - d. **Other GIS Workgroup Activities:** Also underway: Peer-to-peer outreach with counties that have not yet submitted data to the DPS NG9-1-1 database; Best practices and/or resource materials development for edgematching data, required match rates, and data submission schemas.
8. **Staff Notes:**
 - a. **MESB GIS Specialist,** Elizabeth Spracher-Moore, will be getting married in September. Her name will change to Elizabeth Clausen. Notification of her new email address will come in a Friday communication from Jake Jacobson.
 - b. **MESB 9-1-1 Coordinator,** Marcia Broman, retires effective October 31, 2024 after over 40 years of service in the 9-1-1 industry.

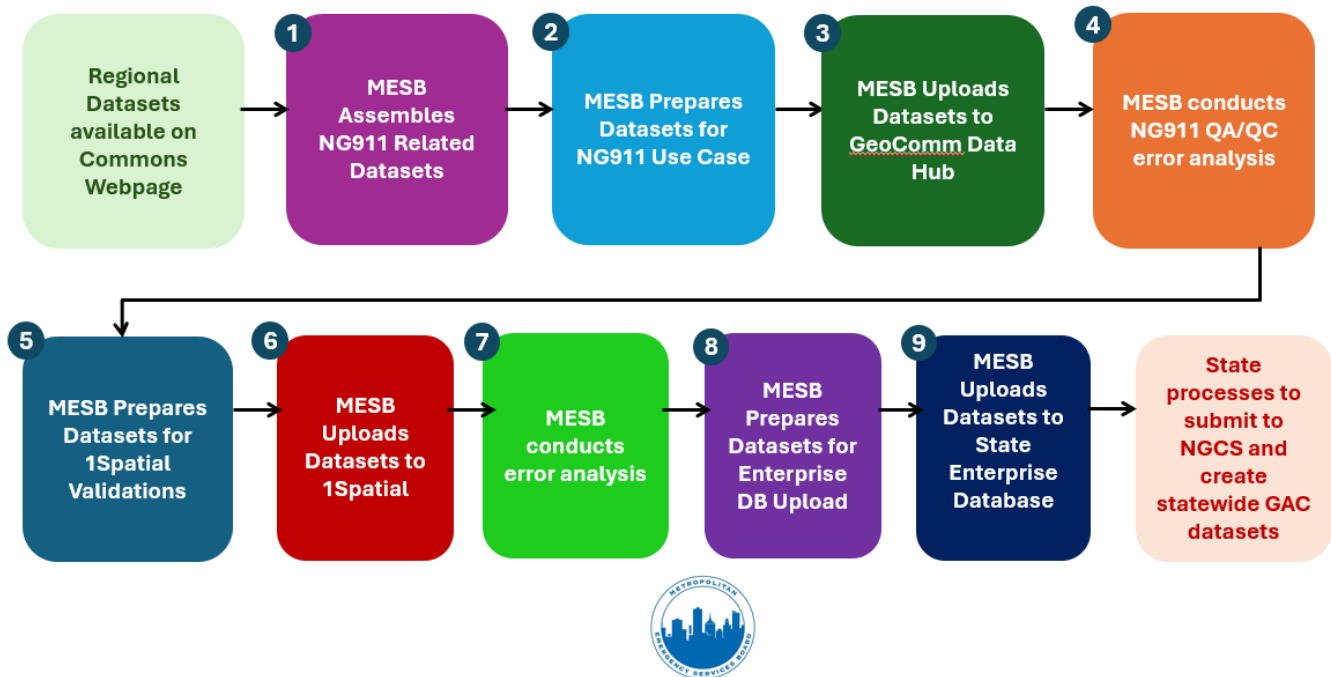
ONGOING ACTIVITIES

9. **Regional GIS Data Aggregation:**
 - a. **Road Centerline and Address Points:** MetroGIS/Met Council processes regional road centerline and address point dataset updates nightly to the MN Geospatial Commons website. Each metro county's most recent centerline and address point data that has been uploaded to the portal and passed validations is included in the regional datasets. The regional road centerline and address point datasets comply with the current MN Geospatial Advisory Council (GAC) data standards.
 - b. **Boundary Polygons:** MESB maintains the regional PSAP, ESZ, MSAG community, law, fire, and EMS boundary polygon layers in coordination with the PSAPs. At least quarterly, Mobile Positioning Center, Text Control Center, and VoIP Positioning Center vendors are directed to the MN Geospatial Commons for downloads of metro's PSAP boundary polygons. This includes the MN State Patrol PSAP boundaries in the MESB region for wireless call Location Based Routing (LBR), as well as routing of Text-to-911 messages.
10. **Regional Data Viewer:** PSAPs are encouraged to use the [Metro Regional Dataviewer](#) developed by MetroGIS/Met Council to view the geospatial data county GIS departments consider valid and current for regional 9-1-1 use. This is the authoritative source of NG9-1-1 GIS data for the 10-county MESB region.
11. **GIS supporting RapidDeploy Radius ALI Mapping:** MESB continues regular monthly "refreshes" of the metro GIS datasets used for ESRI map and geocoding services supporting RapidDeploy Radius mapping system used at many metro PSAPs.
12. **Integration with State NG9-1-1 GIS Activities:**
 - a. All MESB regional NG9-1-1 required datasets are included in the **MN DPS NG9-1-1 enterprise database**, including: the metro regional supplier boundary, road centerlines, address points, and emergency service boundary polygons.
 - b. **Metro Regional GIS datasets are shared publicly** on the [MN Geospatial Commons](#). (See resources under the MetroGIS and MESB organizations on the Commons.) In addition, the regional data is also included as **part of the [MN Road Centerline](#) and [MN Address Point](#) datasets (Opt-In Open Data Counties)**.

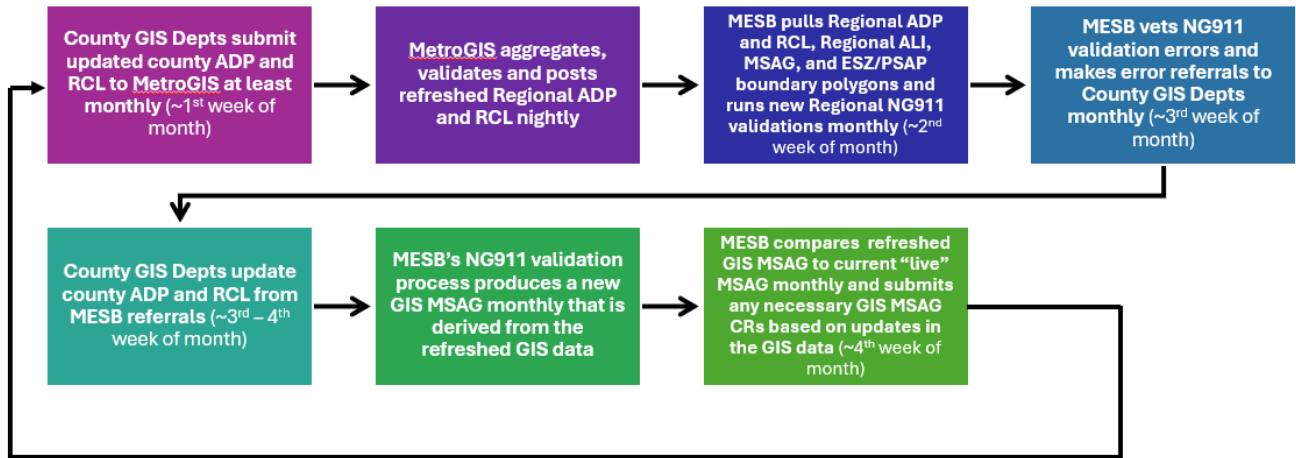
REGIONAL NG911 GIS DATA PROVISIONING



MESB ACTIVITIES supporting REGIONAL NG911 WORKFLOW



Monthly Cadence of Regional NG911 Data Maintenance



**Metropolitan Emergency Services Board
9-1-1 Technical Operations Committee
9-1-1 Network Report
September 2024 Meeting**

MN NG911 RFP Status – Pending

While with the NG911RFP committee, things to note about the existing MESB ESInet environment:

- All PSAPs in the metro have IP connections to the ECN ESInet (not the case in greater MN).
 - Either ...
 - Directly connected to the ESInet.
 - Connecting to Hosts in shared systems that are directly connected to the ESInet.
 - Connected via Motorola SaaS in which hosts (Woodbury, Willmar) are directly connected.
- As PSAPs change to geo-diverse environments, fiber is replacing T1 connections.
 - In general, fiber is preferred for better quality and greater capacity, though existing capacity is sufficient for voice and text bandwidth needs.
- Increase use of MN.IT for carrier diversity.
 - While in general, Lumen has excellent physical diversity in the metro area and can reach ~90% of the metro PSAPs with two diverse circuits, there can be an advantage of having carrier diversity. MN.IT became engaged in the metro as PSAPs upgraded to geo-diverse configurations.
- The SIP (Session Internet Protocol) currently used is RFAI (Request for Assistance Interface) which will need to change to be i3 compatible.
 - What does RFAI mean for us? RFAI is a compatible approach for retrieving ALI data as it's not incorporated with the voice (transmitted as a stream of data packets). With i3 PIDF-LO, ALI data will be encapsulated with the voice. Use of RFAI for ALI lookup made sense when rolling out the ESInet beginning in 2009, but the next ESInet upgrade will have the appropriate SIP "flavor" to accommodate PIDF-LO.
 - As it stands, we're in a chicken vs egg situation: Network hasn't been updated because nearly all carriers have yet to incorporate PIDF-LO; carriers haven't updated because networks aren't ready to handle PIDF-LO. The most likely path for success requires FCC mandates.
- While espoused that the i3 ESInet network will handle video and other non-voice/text inputs, nothing is envisioned in MN or elsewhere in the US.
 - Applications like Prepared Live, RapidDeploy and RapidSOS using separate "Over-the-Top" secure Internet networks will be the only realistic solution for PSAPs to receive such type of inputs for many years.
 - The only other possibility to consolidate multiple feeds will be in the integration with CHE, such as Vesta, Viper and Solacom. Perhaps possible but could bring its own set of issues, notably cybersecurity risks. There isn't visible interest in the industry to go in this direction but wouldn't be surprising if ultimately pursued, though years from hitting the market.

**Metropolitan Emergency Services Board
9-1-1 Technical Operations Committee
9-1-1 Network Report
September 2024 Meeting**

At the writing of this report Sherburne County is scheduled to migrate to a geo-diverse environment September 18.

- As other PSAPs have done or are planning to with a geo-diverse environment, the current location becomes the backup location and the new location becomes the prime staffing location for PSTs.
- Observation: 75% of the Metro PSAPs are or soon plan to be in geo-diverse environments.
- Opinion: Given the supporting populace of the other 25%, it will not make sense for these PSAPs to pursue a geo-diverse environment unless joining into a shared system.

With the exception of Dakota911, there wasn't a significant metro 911 disruption since the last TOC meeting.

For Dakota, the incident involved the SaaS portion of the 911 network connecting to their PSAP.

While the disruption wasn't as severe as their February 8th incident, it pointed to the need to have the Lumen transport circuit used in the SaaS solution to be replaced, despite a considerable non-recurring charge for provisioning. ECN did approve and this circuit ordering/provisioning for the replacing circuit is underway.

The service disruption pointed to a greater need for clarity of vendor responsibilities between the Lumen, the ESINet provider and Motorola, the SaaS solution provider. ECN is reviewing how best to establish and outline the vendors' responsibilities.

8/9 LanguageLine down for several hours

The disruption sparked an examination of who is on the notification email list as no PSAP received an alert from LanguageLine.

MESB worked with LanguageLine to have all metro area PSAPs to be on the notification list. A few PSAPs are yet to be added as they weren't identified as sharing the account. MESB is working with ECN on getting these remaining PSAPs added.

PSAPs are encouraged to assess the merits of over-the-top text language translators as well as trialing emerging AI transcription translators as either a backup or an eventual prime use replacement to LanguageLine.

Going slow – Migration of metro wireline CO migration to Ingress vendor Sinch.

Wireline is the last call type to move off the Minneapolis/St. Paul Legacy Selective Routers and re-homed to Sinch.

MESB has expressed its frustration to Lumen in how slow the effort has been, and the eagerness of getting this completed as the network needs to move forward with more reliable systems.

**Metropolitan Emergency Services Board
9-1-1 Technical Operations Committee
9-1-1 Network Report
September 2024 Meeting**

Why is this important for PSAPs? It is an infrastructure program and mostly involves needed improvements while essentially keeping the same level of existing service. However, some improvements:

- Easier migration to vendor who will be awarded NG911 i3 routing core.
- Simpler connection design between ingress and core routing, which should help in troubleshooting with vendor handoffs.
- Removal of chronic 911 wireline nuisance calls due to bad grounding in which analog noise can trigger a 911 call through the existing legacy system.
- Removal of publicly accessible phone numbers that reach PSAPs via the 911 ESInet, removing potential TDOS vector threat as well as nuisance robo-calls.

Continuing Review of Network Routing Rules

- Jake working through routing rules (Abandonment, alternate, etc) with each PSAP.

8/15 -- ECN awards contracts to RapidDeploy and RapidSOS for their responses to the “Mapped ALI” RFP

- This Contract is available to the Department of Public Safety and for Cooperative Purchasing Venture (CPV) members which includes the MESB.
- Contract Period is through July 31, 2026 with extension options up to 60 months.
- Contracts were executed with fixed pricing. Pricing offered must match or be lower.
- Details are being covered in a series of meetings, discussions, and presentations through September, and likely to continue through the rest of the year.

Lumen ESInet Amendment 11 (Text pricing) approved; Amendment 12 in progress (renewal)

- Amendment 11 addressed costs (\$2500) associated with PSAP facility moves or significant CHE updates that require a rebuilding and reconfiguration of connecting the text network to the PSAP.
- Amendment 12 to address the NG911 Lumen contract renewal with the existing contract expiring November 30th. A two-year renewal is targeted.

Reminder – Keep Jake informed if having network issues

- Let Jake know if you have a Lumen network ticket or having CHE issues which need escalation.

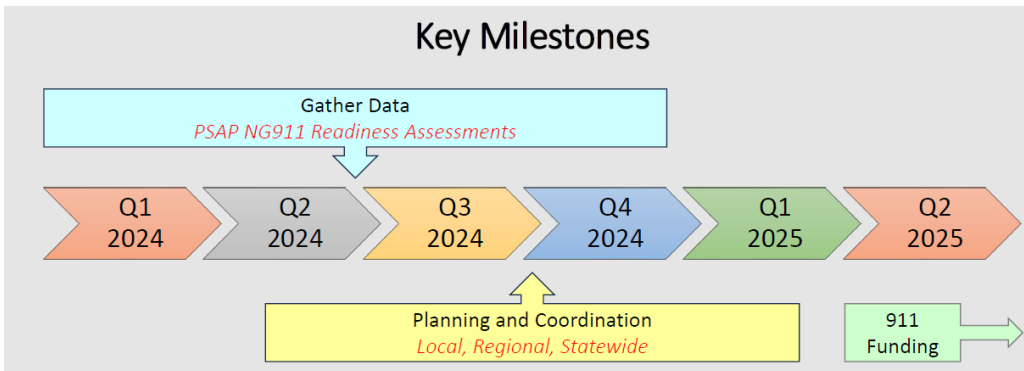
Metropolitan Emergency Services Board 9-1-1 Technical Operations Committee 9-1-1 Network Report September 2024 Meeting

Scheduled by ECN in October

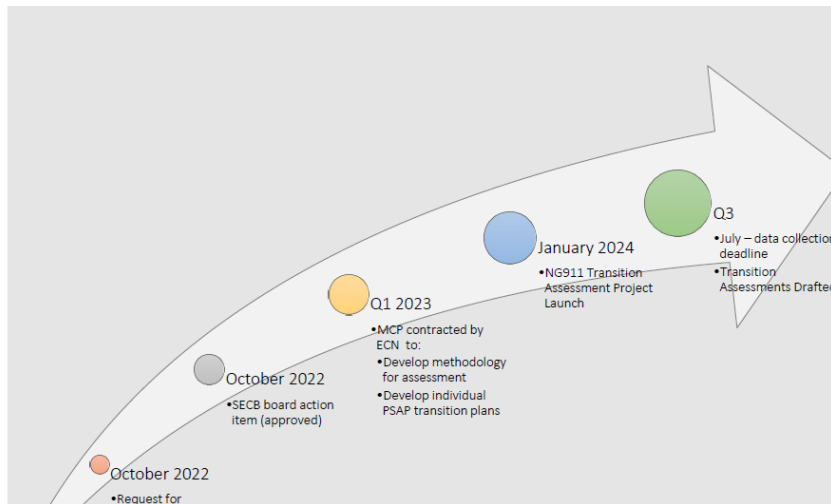
- Assessing PSAP responses from NG911 Data Collection for readiness and potential funding.
- Slides from ECN January 30th presentation

NG911 Transition Planning

Key Milestones



NG911 Transition Planning



Project Timeline

