AT&T Business

161 Inverness Dr W
Englewood CO 80112, USA

Office: 720-628-4605
micah.m.cogan@att.com
www.att.com

February 07, 2020

Dianna Gilliland
The State of Nebraska
State Purchasing Bureau
1526 K Street, Suite 130
Lincoln NE 68508

Dear Ms. Gilliland:

With a large footprint, Nebraska Dept. of Admin Services needs a fast and efficient connection among its various locations in order to handle day-to-day business needs. Therefore, you're looking at connectivity options to enhance your operations.

AT&T understands your priorities and the initiatives that are driving change within your organization. After carefully reviewing your requirements, we propose our cost-effective communication services.

Our proposed solution offers you

- Comprehensive account team support, customer service, and account management
- Streamlined implementation and network management via a single vendor
- Expertise from an experienced account team backed by the resources of one of the world's largest communication companies

With our innovation, experience, and dedication, we're well-positioned to help Nebraska Dept. of Admin Services realize the greatest benefits from its communication network. First, we'll collaborate extensively with you to make sure the service we provide helps you achieve your business objectives. Next, we'll back our services with the ongoing support of an experienced account team.

We're eager to develop our relationship with you, and we look forward to working together on this important project. I'll follow up with you soon to discuss our proposed solution.

Sincerely,

Micah Cogan
Client Solutions Executive

State of Nebraska

Connecting Your World

AT&T Response to The State of Nebraska's RFP #6214 Z1 for Contractual Services

February 07, 2020

Micah Cogan
AT&T
Client Solutions Executive
161 Inverness Dr W
Englewood CO 80112, USA
Office: 720-628-4605
micah.m.cogan@att.com

Proposal Validity Period—The information and pricing contained in this proposal is valid for a period of thirty (30) days from the date written on the proposal cover page unless rescinded or extended in writing by AT&T. **Proposal Pricing**—Pricing proposed herein is based upon the specific product/service mix and locations outlined in this proposal, and is subject to the proposed terms and conditions of AT&T unless otherwise stated herein. Any changes or variations in AT&T proposed terms and conditions and the products, length of term, services, locations, and/or design described herein may result in different pricing. **Copyright Notice and Statement of Confidentiality**—©2020 AT&T Intellectual Property. All rights reserved. AT&T, the Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. The contents of this document are proprietary and confidential and may not be copied, disclose or used, in whole or in part, without the express written permission of AT&T, except to the extent required by law and insofar as is reasonably necessary in order to review and evaluate the information contained herein.

Table of Contents

State of Nebraska i

Executive Summary 4

RFP Response: 7

SCOPE OF SERVICE 7

GLOSSARY OF TERMS 11

I. PROCUREMENT PROCEDURE 19

A. GENERAL INFORMATION 19

B. PROCURING OFFICE AND COMMUNICATION WITH STATE STAFF AND EVALUATORS 19

C. SCHEDULE OF EVENTS 20

D. WRITTEN QUESTIONS AND ANSWERS 21

E. NOTIFICATION OF INTENT TO SUBMIT APROPOSAL 21

F. SECRETARY OF STATE/TAX COMMISSIONER REGISTRATION REQUIREMENTS (Statutory) 22

G. ETHICS IN PUBLIC CONTRACTING 22

H. DEVIATIONS FROM THE REQUEST FOR PROPOSAL 23

I. SUBMISSION OF PROPOSALS 24

J. PROPOSAL PREPARATION COSTS 25

K. FAILURE TO COMPLY WITH REQUEST FOR PROPOSAL 25

L. PROPOSAL CORRECTIONS 26

M. LATE PROPOSALS 26

N. PROPOSAL OPENING 27

O. REQUEST FOR PROPOSAL/PROPOSAL REQUIREMENTS 27

P. EVALUATION COMMITTEE 28

Q. EVALUATION OF PROPOSALS 28

R. COST CLARIFICATION 30

S. ORAL INTERVIEWS/PRESENTATIONS AND/OR DEMONSTRATIONS 31

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

T. BEST AND FINAL OFFER 31
U. REFERENCE AND CREDIT CHECKS 32
V. AWARD 32
W. ALTERNATE/EQUIVALENT PROPOSALS 33
X. LUMP SUM OR "ALL OR NONE" PROPOSALS 34
Y. EMAIL SUBMISSIONS 34
Z. REJECTION OF PROPOSALS 34
AA. RESIDENT BIDDER 35
II. TERMS AND CONDITIONS 36
A. GENERAL 38
B. NOTIFICATION 39
C. NOTICE (POC) 39
D. GOVERNING LAW (Statutory) 40
E. BEGINNING OF WORK 40
F. AMENDMENT 41
G. CHANGE ORDERS OR SUBSTITUTIONS 41
H. VENDOR PERFORMANCE REPORT(S) 42
I. NOTICE OF POTENTIAL CONTRACTOR BREACH 43
J. BREACH 43
K. NON-WAIVER OF BREACH 44
L. SEVERABILITY 45
M. INDEMNIFICATION 45
N. ATTORNEY'S FEES 47
O. ASSIGNMENT, SALE, OR MERGER 47
P. CONTRACTING WITH OTHER NEBRASKA POLITICAL SUB-DIVISIONS OF THE STATE OR ANOTHER STATE 48
Q. FORCE MAJEURE 49
R. CONFIDENTIALITY 49
S. EARLY TERMINATION 50
T. CONTRACT CLOSEOUT 51

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

III. CONTRACTOR DUTIES 53
A. INDEPENDENT CONTRACTOR /OBLIGATIONS 53
B. EMPLOYEE WORK ELIGIBILITY STATUS 55
C. COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory) 56
D. COOPERATION WITH OTHER CONTRACTORS 57
E. DISCOUNTS 57
F. PRICES 58
G. PERMITS, REGULATIONS, LAWS 59
H. OWNERSHIP OF INFORMATION AND DATA /DELIVERABLES 59
I. INSURANCE REQUIREMENTS 60
J. NOTICE OF POTENTIAL CONTRACTOR BREACH 64
K. ANTITRUST 64
L. CONFLICT OF INTEREST 65
M. STATE PROPERTY 66
N. SITE RULES AND REGULATIONS 66
O. ADVERTISING 67
P. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory) 67
Q. DISASTER RECOVERY/BACK UP PLAN 68
R. DRUG POLICY 68
S. WARRANTY 71
IV. PAYMENT 72
A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory) 72
B. TAXES (Statutory) 72
C. INVOICES 72
D. INSPECTION AND APPROVAL 73
E. PAYMENT (Statutory) 73
F. LATE PAYMENT (Statutory) 74
G. SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS (Statutory) 74

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

H. RIGHT TO AUDIT (First Paragraph is Statutory) 74
V. PROJECT DESCRIPTION AND SCOPE OF WORK 76
A. PROJECT OVERVIEW 76
B. PROJECT ENVIRONMENT 76
C. SCOPE OF WORK 79
D. TECHNICAL REQUIREMENTS 80
E. DELIVERABLES 80
VI. PROPOSAL INSTRUCTIONS 80
A. PROPOSAL SUBMISSION 81
Form A Contractor Proposal Point of Contact 89
Form B Notification of Intent to Submit Proposal 90
REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM 91
AT&T Attachments: 93
- State of Nebraska WSCA 93
- Master Service Agreement_fe 93
- Business_Continuity_Handbook 93

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Notwithstanding anything contained in this State of Nebraska (the "State") Request for Proposal No. 6214 Z1 ("RFP") Mass Notification Service (MNS) to the contrary, AT&T Mobility National Accounts LLC ("AT&T") submits this response to the RFP ("Response") subject to the provisions of this Response and the terms and conditions in the Western States Contracting Alliance d/b/a "NASPO ValuePoint" (formerly known as "WSCA" or "WSCA-NASPO") Master Service Agreement #1907, dated March 15, 2012 (the "NASPO/WSCA Master Agreement"), together with the corresponding State of Nebraska Participating Addendum and Contract 55001 04 executed on February 4, 2013, as amended (the "State of Nebraska PA") (collectively, the "NASPO/WSCA 3 Contract"). The NASPO/WSCA Master Agreement, the State of Nebraska PA and any associated transaction-specific documents to be entered into between the parties are collectively referred to throughout this Response as the "Proposed Contract Documents."

The AT&T NASPO/WSCA Master Agreement along with Nebraska PA, is currently scheduled to expire on December 31, 2020; therefore, proposed services under this Response for additional years are contingent on AT&T being selected by NASPO/WSCA as one of its vendors on a going forward basis. If so selected by NASPO/WSCA, AT&T will migrate the State to rates, terms and conditions consistent with the new NASPO/WSCA agreement and the new related Participating Addendum for the remaining term of the final agreement between the parties. Revised documentation may be required to transition the State to the new NASPO/WSCA agreement. In the event material changes between the current and future NASPO/WSCA serving arrangements exist, the State may terminate the applicable AT&T Service with no penalty upon the expiration of the existing NASPO/WSCA Master.

The NASPO/WSCA 3 Contract is a customized contract that allows AT&T to offer robust pricing to customers such as the State. The favorable pricing submitted by this Response, assumes that the State will agree to use the NASPO/WSCA 3 Contract in any final, negotiated contract between the parties in connection with an award to AT&T under this RFP. AT&T's Response is conditioned on the State's willingness to agree to the terms and conditions of the Proposed Contract Documents for the provision of the services requested by this RFP to be provided by AT&T. Except as may be specifically clarified by AT&T in this Response, AT&T takes exception to the terms or conditions contained in the RFP that are inconsistent with the Proposed Contract Documents. This exception is taken regardless of whether AT&T has specifically referenced the Proposed Contract Documents in response to any individual provision in the RFP. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer. You can find more about AT&T's offers at the AT&T WSCA Program Information website: http://www.wireless.att.com/businesscenter/legal-contracts/wsca.jsp

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Any software used with the Services will be governed by the written terms and conditions applicable to such software. Title to software remains with AT&T or its supplier. The State must comply with all such terms and conditions, and they shall take precedence over any agreement between the parties as relates to such software.

Submission of this proposal does not obligate either party to enter into a contract of any kind, create legal obligations on the part of either party or obligate either party to pay expenses incurred by the other party. Any agreement between the parties must be in writing and signed by both parties after finalization of appropriate terms and conditions.

Any changes, additions or deletions to the products, services, quantities, revenue commitments, or term of the proposed arrangement may result in changes to the rates, discounts, credits or other terms contained in this Response.

AT&T respectfully requests that information in this document be held confidential by the State to the extent allowed under applicable law.

Proposal Validity Period—The information and pricing contained in this proposal is valid for a period of ninety (90) days from the date written on the proposal cover page unless rescinded or extended in writing by ***AT&T.***

Proposal Pricing—Pricing proposed herein is based upon the specific product/service mix and locations outlined in this proposal unless otherwise stated herein. Any changes or variations in the proposed terms and conditions, the products/services, length of term, locations, and/or design described herein may result in different pricing. Prices quoted do not include applicable taxes, surcharges, or fees. In accordance with the tariffs or other applicable service agreement terms, customer is responsible for payment of such charges.

Providers of Service—Subsidiaries and affiliates of AT&T Corp. provide products and services under the AT&T brand.

Copyright Notice and Statement of Confidentiality—© 2020 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo, and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. AT&T respectfully requests that information in this document be held confidential by the State to the extent allowed under applicable law.

Coverage is not available in all areas. AT&T wireless coverage maps are available at www.wireless.att.com/coverageviewer. Wireless service is subject to transmission limitations and terrain, system, capacity and other limitations. Availability, security,

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T. When outside coverage area, access will be limited to information and applications previously downloaded to or resident on your device.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Executive Summary

To address citizen needs, states must improve efficiencies, upgrade technologies, and find creative ways to deliver services on a tight budget. Therefore, states like yours need to align operating practices with evolving technologies.

Nebraska Dept. of Admin Services must have an infrastructure in place that will support operations and future objectives effectively. You want a supplier that can help you build a network platform to support these objectives:

- Reduce your operational risk
- Improve performance
- Increase the productivity and efficiency of your staff
- Enhance the services that you provide

We understand your organization's challenges and the technologies that drive your business. As a result, we've devised a solution and responded to your RFP with details about each of the services you need. Our solution includes services that can help enable you to upgrade your technology and gain additional efficiencies, which can help streamline your communications.

Solution

Our solution for Nebraska Dept. of Admin Services is a good value and a smart investment. This is because we designed it based on your needs now—and so that you can easily add other services when you're ready.

We have collaborated with RAVE Mobile Solutions to build the solution that empowers you partner with your community to save lives. Our solutions will allow you to collaborate across agencies to leverage all your data and communications for a coordinated response. This scalable platform sends external and internal mass notifications and provides critical real-time incident information to 9-1-1 call takers and first responders. The RAVE solutions help communities continue increasing efficiency and protecting residents, visitors, vulnerable populations and first responders.

The solution has these key features:

- **Beyond Community Mass Notification**—Improve citizen engagement with community alerts that can leverage citizen-provided data to send targeted messages and initiate two-way texting to get feedback during critical events.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

- **Mobile Soft Target Protection**—Leverage mobile technology to enable fast action by staff and bystanders in soft target locations to send in anonymous tips or trigger a panic button activation to 9-1-1 and on-site security personnel.
- **Vulnerable and Functional Needs Registry**- Help emergency managers understand the individual needs in their community and enable faster communication during a disaster with a web-based, citizen provided vulnerable and functional needs registry.
- **Enhanced Situational Awareness Data-** Equip first responders with accurate site details, such as floor plans, utility shutoff locations, hazardous material and AED locations during 9-1-1 calls, and as part of a searchable critical infrastructure database.

Advantages of AT&T

- **Government Experience**—We provide services to many state and local governments, which gives us a better understanding of your unique needs. We have more than 4,000 employees who support Public Sector entities and know what it takes to manage government networks and infrastructure.
- **Customer Experience and Satisfaction**—Building strong customer relationships is one of our core values. We want you to have an effortless experience. That's why we offer you convenient ways to contact us and get support for your AT&T services, including online and application-based support tools; customer service in more than 160 languages; and teams of sales, customer care, and technical support specialists to help you. We constantly strive to improve processes such as pricing, contracting, ordering, provisioning, and billing. Our efforts have resulted in better order quality, faster installation, faster repair times, and more accurate billing.

Personalized Support

Because we understand the importance of personalized service, we give you an account team of specialists to design and implement your new solution. You'll receive ongoing, coordinated support from your account team for all of your AT&T services.

Your Account Team

Name	Title	Phone Number	Email
Micah Cogan	Client Solutions Executive	720-628-4605	micah.m.cogan@att.com
Chris Wilson	Regional Sales Manager	618-604-9063	cw3543@att.com

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

You'll see from our proposal that we understand your objectives and have the expertise and resources to support them. We look forward to working with you to help you reach your goals.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

RFP Response:

State of Nebraska
REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES

RETURN TO:
State Purchasing Bureau
1526 K Street, Suite 130
Lincoln, NE 68508
Phone: 402-471-6500

RFP NUMBER	RELEASE DATE
RFP 6214 Z1	January 13, 2020
OPENING DATE AND TIME	PROCUREMENT CONTACT
February 7, 2020, 2:00 p.m. Central Time	Dianna Gilliland/Julie Schiltz

PLEASE READ CAREFULLY!

SCOPE OF SERVICE

The State of Nebraska (State), Department of Administrative Services (DAS), Materiel Division, State Purchasing Bureau (SPB), is issuing this Request for Proposal (RFP) Number 6214 Z1 for the purpose of selecting a qualified Bidder to provide Mass Notification Service (MNS). A more detailed description can be found in Section V. The resulting contract may not be an exclusive contract as the State reserves the right to contract for the same or similar services from other sources now or in the future.

The term of the contract will be three (3) years commencing upon execution of the contract by the State and the Contractor (Parties). The Contract includes the option to renew for five (5) additional one (1) year periods upon mutual agreement of the Parties. The State reserves the right to extend the period of this contract beyond the termination date when mutually agreeable to the Parties.

AT&T Response:

The AT&T NASPO/WSCA Master Agreement along with Nebraska PA, is currently scheduled to expire on December 31, 2020; therefore, proposed services under this Response for additional years are contingent on AT&T being selected by NASPO/WSCA as one of its vendors on a going forward basis. If so selected by NASPO/WSCA, AT&T will migrate the State to rates, terms and conditions consistent with the new NASPO/WSCA agreement and the new related Participating Addendum for the remaining term of the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

final agreement between the parties. Revised documentation may be required to transition the State to the new NASPO/WSCA agreement. In the event material changes between the current and future NASPO/WSCA serving arrangements exist, the State may terminate the applicable AT&T Service with no penalty upon the expiration of the existing NASPO/WSCA Master.

ALL INFORMATION PERTINENT TO THIS REQUEST FOR PROPOSAL CAN BE FOUND ON THE INTERNET AT: **http://das.nebraska.gov/materiel/purchasing.html.**

IMPORTANT NOTICE: Pursuant to Neb. Rev. Stat. § 84-602.04, State contracts in effect as of January 1, 2014, and contracts entered into thereafter, must be posted to a public website. The resulting contract, the RFP, and the successful contractor's proposal or response will be posted to a public website managed by DAS, which can be found at **http://statecontracts.nebraska.gov.**

In addition and in furtherance of the State's public records Statute (Neb. Rev. Stat. § 84-712 et seq.), all proposals or responses received regarding this RFP will be posted to the State Purchasing Bureau public website.

These postings will include the entire proposal or response. Bidder must request that proprietary information be excluded from the posting. The bidder must identify the proprietary information, mark the proprietary information according to state law, and submit the proprietary information in a separate container or envelope marked conspicuously using an indelible method with the words "PROPRIETARY INFORMATION". The bidder must submit a detailed written document showing that the release of the proprietary information would give a business advantage to named business competitor(s) and explain how the named business competitor(s) will gain an actual business advantage by disclosure of information. The mere assertion that information is proprietary or that a speculative business advantage might be gained is not sufficient. (See Attorney General Opinion No. 92068, April 27, 1992) THE SUPPLIER MAY NOT ASSERT THAT THE ENTIRE PROPOSAL IS PROPRIETARY. COST PROPOSALS WILL NOT BE CONSIDERED PROPRIETARY AND ARE A PUBLIC RECORD IN THE STATE OF NEBRASKA. The State will then determine, in its discretion, if the interests served by nondisclosure outweighs any public purpose served by disclosure. (See Neb. Rev. Stat. § 84-712.05(3)) The Bidder will be notified of the agency's decision. Absent a State determination that information is proprietary, the State will consider all information a public record subject to release regardless of any assertion that the information is proprietary.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

If the agency determines it is required to release proprietary information, the bidder will be informed. It will be the bidder's responsibility to defend the contractor's asserted interest in non-disclosure.

AT&T Response:

AT&T respectfully requests that information in this document be held confidential by the State to the extent allowed under applicable law.

To facilitate such public postings, with the exception of proprietary information, the State of Nebraska reserves a royalty-free, nonexclusive, and irrevocable right to copy, reproduce, publish, post to a website, or otherwise use any contract, proposal, or response to this RFP for any purpose, and to authorize others to use the documents. Any individual or entity awarded a contract, or who submits a proposal or response to this RFP, specifically waives any copyright or other protection the contract, proposal, or response to the RFP may have; and, acknowledges that they have the ability and authority to enter into such waiver. This reservation and waiver is a prerequisite for submitting a proposal or response to this RFP, and award of a contract. Failure to agree to the reservation and waiver will result in the proposal or response to the RFP being found non- responsive and rejected.

AT&T Response:

AT&T agrees that the physical response materials become the property of the State. However, any intellectual property of AT&T, AT&T manufacturers or other third parties included in AT&T's Response will remain the property of the respective owner and no title shall transfer by disclosure of such intellectual property as part of AT&T's Response. AT&T further agrees that the State may use its RFP Response as needed in connection with this RFP and the analysis of the AT&T Proposal; provided that AT&T's Proposal may not be shared with third party vendors competing for this RFP and that the State will protect AT&T's Proposal as a confidential document under the terms of applicable open records policies and laws.

AT&T clarifies that all intellectual property in items arising by virtue of AT&T's performance of the Services will be the sole and exclusive property of AT&T. The State will own copies of any reports produced and furnished to the State by AT&T in providing the Service and will be granted under AT&T's copyrights, a perpetual, non-exclusive, personal and non-transferable right to reproduce and modify any such reports for the State's own internal business purposes.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Any entity awarded a contract or submitting a proposal or response to the RFP agrees not to sue, file a claim, or make a demand of any kind, and will indemnify and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials from and against any and all claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses, sustained or asserted against the State, arising out of, resulting from, or attributable to the posting of the contract or the proposals and responses to the RFP, awards, and other documents.

AT&T Response:

AT&T's Response is submitted pursuant to this Response and subject to the terms and conditions of the Proposed Contract Documents. All terms and conditions regarding Indemnification are set forth Section 25 ("Indemnification") of the NASPO/WSCA Master Agreement. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

GLOSSARY OF TERMS

AT&T Response:

AT&T's Response is submitted pursuant to this Response and subject to the terms of the Proposed Contract Documents. The NASPO/WSCA 3 Contract is a customized contract that allows AT&T to offer robust pricing to customers such as the State. The favorable pricing submitted by this Response, assumes that the State will agree to use the NASPO/WSCA 3 Contract in any final, negotiated contract between the parties in connection with an award to AT&T under this RFP. AT&T's Response is conditioned on the State's willingness to agree to the terms and conditions of the Proposed Contract Documents for the provision of the services requested by this RFP to be provided by AT&T. Except as may be specifically clarified by AT&T in this Response, AT&T takes exception to the terms or conditions contained in the RFP that are inconsistent with the Proposed Contract Documents. This exception is taken regardless of whether AT&T has specifically referenced the Proposed Contract Documents in response to any individual provision in the RFP. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer.

Acceptance Test Procedure: Benchmarks and other performance criteria, developed by the State of Nebraska or other sources of testing standards, for measuring the effectiveness of products or services and the means used for testing such performance.

Addendum: Something to be added or deleted to an existing document; a supplement.

Administrative Services: An agency of the State of Nebraska.

After Receipt of Order (ARO): After Receipt of Order

Agency: Any state agency, board, or commission other than the University of Nebraska, the Nebraska State colleges, the courts, the Legislature, or any other office or agency established by the Constitution of Nebraska.

Agent/Representative: A person authorized to act on behalf of another.

Amend: To alter or change by adding, subtracting, or substituting.

Amendment: A written correction or alteration to a document.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

API: Application Programming Interface.

Appropriation: Legislative authorization to expend public funds for a specific purpose. Money set apart for a specific use.

Automated Clearing House: (ACH) Electronic network for financial transactions in the United States

Award: All purchases, leases, or contracts which are based on competitive proposals will be awarded according to the provisions in the RFP.

Best and Final Offer (BAFO): In a competitive proposal, the final offer submitted which contains the contractor's most favorable terms for price.

Bid Bond: An insurance agreement, accompanied by a monetary commitment, by which a third party (the surety) accepts liability and guarantees that the contractor will not withdraw the bid.

Bidder: A vendor who submits a proposal in response to a written RFP.

Breach: Violation of a contractual obligation by failing to perform or repudiation of one's own promise.

Business: Any corporation, partnership, individual, sole proprietorship, joint-stock company, joint venture, or any other private legal entity.

Business Day: Any weekday, except State-recognized holidays.

Calendar Day: Every day shown on the calendar including Saturdays, Sundays, and State/Federal holidays. **Cancellation:** To call off or revoke a purchase order without expectation of conducting or performing it at a later time. **CAP:** Common Alerting Protocol.

Change Order: Document that provides amendments to an executed purchase order or contract.

CMAS: Commercial Mobile Alert System.

Collusion: An agreement or cooperation between two or more persons or entities to accomplish a fraudulent, deceitful, or unlawful purpose.

COI: Certificate of Insurance of Insurance,

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Competition: The effort or action of two or more commercial interests to obtain the same business from third parties.

Confidential Information: Unless otherwise defined below, "Confidential Information" shall also mean proprietary trade secrets, academic and scientific research work which is in progress and unpublished, and other information which if released would give advantage to business competitors and serve no public purpose (see Neb. Rev. Stat. §84-712.05(3)). In accordance with Nebraska Attorney General Opinions 92068 and 97033, proof that information is proprietary requires identification of specific, named competitor(s) who would be advantaged by release of the information and the specific advantage the competitor(s) would receive.

Contract: An agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law; the writing that sets forth such an agreement.

Contract Administration: The administration of the contract which includes and is not limited to; contract signing, contract amendments and any necessary legal actions.

Contract Award: Occurs upon execution of the State document titled "Service Contract Award" by the proper authority.

Contract Management: The management of day to day activities at the agency which includes and is not limited to ensuring deliverables are received, specifications are met, handling meetings and making payments to the Contractor.

Contract Period: The duration of the contract.

Contractor: An individual or entity lawfully conducting business in the State, or licensed to do so, who seeks to provide goods or services under the terms of a written RFP.

Copyright: A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt and distribute the work.

Critical Program Error: Any Program Error, whether or not known to the State, which prohibits or significantly impairs use of the Licensed Software as set forth in the documentation and intended in the contract.

CSV: Coma Separated Values.

Customer Service: The process of ensuring customer satisfaction by providing assistance and advice on those products or services provided by the Contractor.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Default: The omission or failure to perform a contractual duty.

DAS: Department of Administrative Services.

Deviation: Any proposed change(s) or alteration(s) to either the terms and conditions or deliverables within the scope of the written RFP or contract.

DHS: Department of Homeland Security.

ENS: Emergency Notification Service.

Evaluation: The process of examining an offer after opening to determine the bidder's responsibility, responsiveness to requirements, and to ascertain other characteristics of the offer that relate to determination of the successful award.

Evaluation Committee: Committee(s) appointed by the requesting agency that advises and assists the procuring office in the evaluation of proposals (offers made in response to written RFPs).

Extension: Continuance of a contract for a specified duration upon the agreement of the parties beyond the original Contract Period. Not to be confused with "Renewal Period".

FEMA: Federal Emergency Management Agency.

Free on Board (F.O.B.) Destination: The delivery charges are included in the quoted price and prepaid by the contractor. Contractor is responsible for all claims associated with damages during delivery of product.

Free on Board (F.O.B.) Point of Origin: The delivery charges are not included in the quoted price and are the responsibility of the agency. Agency is responsible for all claims associated with damages during delivery of product.

Foreign Corporation: A foreign corporation that was organized and chartered under the laws of another state, government, or country.

GIS: Geographic Information Systems.

Installation Date: The date when the procedures described in "Installation by Contractor", and "Installation by State", as found in the RFP, or contract, are completed.

Interested Party: A person, acting in their personal capacity, or an entity entering into a contract or other agreement creating a legal interest therein.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Invalid Proposal: A proposal that does not meet the requirements of the RFP or cannot be evaluated against the other proposals.

IPAWS: Integrated Public Alert Warning System.

Late Proposal: An offer received after the Opening Date and Time.

Licensed Software Documentation: The user manuals and any other materials in any form or medium customarily provided by the Contractor to the users of the Licensed Software which will provide the State with sufficient information to operate, diagnose, and maintain the Licensed Software properly, safely, and efficiently.

Mandatory/Must: Required, compulsory, or obligatory. **May:** Discretionary, permitted; used to express possibility. **MNS:** Mass Notification Service.

Module (see System): A collection of routines and data structures that perform a specific function of software.

Must: See Mandatory/Must and Shall/Will/Must.

NSA: National Security Agency.

NWS: National Weather Service.

OCIO: Office of the Chief Information Officer, a division of Administrative Services, an agency of the State of Nebraska.

Open Market Purchase: Authorization may be given to an agency to purchase items above direct purchase authority due to the unique nature, price, quantity, location of the using agency, or time limitations by the AS Materiel Division, State Purchasing Bureau.

Opening Date and Time: Specified date and time for the public opening of received, labeled, and sealed formal proposals.

Operating System: The control program in a computer that provides the interface to the computer hardware and peripheral devices, and the usage and allocation of memory resources, processor resources, input/output resources, and security resources.

Outsourcing: The contracting out of a business process which an organization may have previously performed internally or has a new need for, to an independent organization from which the process is purchased back.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Payroll & Financial Center (PFC): State of Nebraska's electronic procurement system of record.

Performance Bond: An insurance agreement, accompanied by a monetary commitment, by which a third party (the surety) accepts liability and guarantees that the Contractor fulfills any and all obligations under the contract.

PII: Personally Identifiable Information.

PIN: Personal Identification Number.

Platform: A specific hardware and Operating System combination that is different from other hardware and Operating System combinations to the extent that a different version of the Licensed Software product is required to execute properly in the environment established by such hardware and Operating System combination.

Point of Contact (POC): The person designated to receive communications and to communicate.

Pre-Proposal Conference: A meeting scheduled for the purpose of clarifying a written RFP and related expectations.

Product: Something that is distributed commercially for use or consumption and that is usually (1) tangible personal property, (2) the result of fabrication or processing, and (3) an item that has passed through a chain of commercial distribution before ultimate use or consumption.

Program Error: Code in Licensed Software which produces unintended results or actions, or which produces results or actions other than those described in the specifications. A program error includes, without limitation, any Critical Program Error.

Program Set: The group of programs and products, including the Licensed Software specified in the RFP, plus any additional programs and products licensed by the State under the contract for use by the State.

Project: The total scheme, program, or method worked out for the accomplishment of an objective, including all documentation, commodities, and services to be provided under the contract.

Proposal: An offer, bid, or quote submitted by a contractor/vendor in a response to a written RFP

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Proprietary Information: Proprietary information is defined as trade secrets, academic and scientific research work which is in progress and unpublished, and other information which if released would give advantage to business competitors and serves no public purpose (see Neb. Rev. Stat. § 84-712.05(3)). In accordance with Attorney General Opinions 92068 and 97033, proof that information is proprietary requires identification of specific named competitor(s) advantaged by release of the information and the demonstrated advantage the named competitor(s) would gain by the release of information.

Protest/Grievance: A complaint about a governmental action or decision related to a RFP or resultant contract, brought by a contractor who has timely submitted a proposal response in connection with the award in question, to AS Materiel Division or another designated agency with the intention of achieving a remedial result.

Public Proposal Opening: The process of opening correctly submitted offers at the time and place specified in the written RFP and in the presence of anyone who wished to attend.

RSS: Really Simple Syndication.

Recommended Hardware Configuration: The data processing hardware (including all terminals, auxiliary storage, communication, and other peripheral devices) to the extent utilized by the State as recommended by the Contractor.

Release Date: The date of public release of the written RFP to seek offers.

Renewal Period: Optional contract periods subsequent to the original Contract Period for a specified duration with previously agreed to terms and conditions. Not to be confused with Extension.

Request for Proposal (RFP): A written RFP utilized for obtaining competitive offers.

Responsible Contractor: A contractor who has the capability in all respects to perform fully and lawfully all requirements with integrity and reliability to assure good faith performance.

Responsive Bidder: A vendor who has submitted a proposal which conforms to all requirements of the RFP document.

Shall/Will/Must: An order/command; mandatory.

Should: Expected; suggested, but not necessarily mandatory.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

SMS: Short Message Service.

Software License: Legal instrument with or without printed material that governs the use or redistribution of licensed software.

Specifications: The detailed statement, especially of the measurements, quality, materials, and functional characteristics, or other items to be provided under a contract.

SPB: State Purchasing Bureau, a division of Administrative Services, an agency of the State of Nebraska.

Statutory: These clauses are controlled by state law and are not subject to negotiation.

Subcontractor: Individual or entity with whom the contractor enters a contract to perform a portion of the work awarded to the contractor.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

I. PROCUREMENT PROCEDURE

A. GENERAL INFORMATION

The RFP is designed to solicit proposals from qualified bidders who will be responsible for providing Mass Notification Service (MNS) at a competitive and reasonable cost. Terms and Conditions, Project Description and Scope of Work, Proposal instructions, and Cost Proposal Requirements may be found in Sections II through VI.

Proposals shall conform to all instructions, conditions, and requirements included in the RFP. Prospective bidders are expected to carefully examine all documents, schedules, and requirements in this RFP, and respond to each requirement in the format prescribed. Proposals may be found non-responsive if they do not conform to the RFP.

AT&T Response:

AT&T has read and understands.

B. PROCURING OFFICE AND COMMUNICATION WITH STATE STAFF AND EVALUATORS

Procurement responsibilities related to this RFP reside with State Purchasing Bureau. The point of contact (POC) for the procurement is as follows:

RFP Number:	6214 Z1
Name:	Dianna Gilliland/Julie Schiltz, Buyer(s)
Agency:	State Purchasing Bureau
Address:	1526 K Street, Suite 130
	Lincoln, NE 68508
Telephone:	402-471-6500
E-Mail:	as.materielpurchasing@nebraska.gov

From the date the RFP is issued until the Intent to Award is issued, communication from the Bidder is limited to the POC listed above. After the Intent to Award is issued, the Bidder may communicate with individuals the State has designated as responsible for negotiating the contract on behalf of the State. No member of the State Government, employee of the State, or member of the Evaluation Committee is empowered to make binding statements regarding this RFP. The POC will issue any answers, clarifications or amendments regarding this RFP in writing. Only the SPB or awarding agency can award a

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

contract. Bidders shall not have any communication with, or attempt to communicate or influence any evaluator involved in this RFP.

The following exceptions to these restrictions are permitted:

1. Contact made pursuant to pre-existing contracts or obligations;
2. Contact required by the schedule of events or an event scheduled later by the RFP POC; and
3. Contact required for negotiation and execution of the final contract.

The State reserves the right to reject a bidder's proposal, withdraw an Intent to Award, or terminate a contract if the State determines there has been a violation of these procurement procedures.

AT&T Response:

AT&T has read and understands.

C. SCHEDULE OF EVENTS

The State expects to adhere to the procurement schedule shown below, but all dates are approximate and subject to change.

	ACTIVITY	DATE/TIME
1.	Release RFP	January 13, 2020
2.	Last day to submit written questions	January 24, 2020
3.	State responds to written questions through RFP "Addendum" and/or "Amendment" to be posted to the Internet at: and http://das.nebraska.gov/materiel/purchasing.html	January 30, 2020
4.	Proposal Opening Location: State Purchasing Bureau 1526 K Street, Suite 130 Lincoln, NE 68508	February 7, 2020 2:00 PM Central Time
5.	Review for conformance to RFP requirements	February 7, 2020
6.	Evaluation period	February 10-14, 2020
7.	"Oral Interviews/Presentations and/or Demonstrations" (if required)	February 27, 2020
8.	Post "Notification of Intent to Award" to Internet at: http://das.nebraska.gov/materiel/purchasing.html	March 2, 2020
9.	Contract finalization period	March 2, 2020 through March 31, 2020

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

	ACTIVITY	DATE/TIME
10.	Contract award	April 1, 2020
11.	Contractor start date	April 16, 2020

AT&T Response:

AT&T has read and understands.

D. WRITTEN QUESTIONS AND ANSWERS

Questions regarding the meaning or interpretation of any RFP provision must be submitted in writing to State Purchasing Bureau and clearly marked "RFP Number 6214 Z1; Mass Notification Service (MNS) Questions". The POC is not obligated to respond to questions that are received late per the Schedule of Events.

Bidders should present, as questions, any assumptions upon which the Bidder's proposal is or might be developed. Proposals will be evaluated without consideration of any known or unknown assumptions of a bidder. The contract will not incorporate any known or unknown assumptions of a bidder.

It is preferred that questions be sent via e-mail to as.materielpurchasing@nebraska.gov, but may be delivered by hand or by U.S. Mail. It is recommended that Bidders submit questions using the following format.

RFP Section Reference	RFP Page Number	Question

Written answers will be posted at http://das.nebraska.gov/materiel/purchasing.html per the Schedule of Events.

AT&T Response:

AT&T has read and understands.

E. NOTIFICATION OF INTENT TO SUBMIT APROPOSAL

Bidders who intend to submit a proposal should complete a "Notification of Intent to Submit a Proposal Form" (see Form B) and deliver the form by hand or U.S. mail to the POC for the RFP per the Schedule of Events. A list of bidders who submitted a

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Notification of Intent to Submit a Proposal will be posted on the Internet at http://das.nebraska.gov/materiel/purchasing.html.

AT&T Response:

AT&T has read and understands.

F. SECRETARY OF STATE/TAX COMMISSIONER REGISTRATION REQUIREMENTS (Statutory)

All bidders must be authorized to transact business in the State of Nebraska and comply with all Nebraska Secretary of State Registration requirements. The bidder who is the recipient of an Intent to Award may be required to certify that it has complied and produce a true and exact copy of its current (within ninety (90) calendar days of the intent to award) Certificate or Letter of Good Standing, or in the case of a sole proprietorship, provide written documentation of sole proprietorship and complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html. This must be accomplished prior to execution of the contract.

G. ETHICS IN PUBLIC CONTRACTING

The State reserves the right to reject proposals, withdraw an intent to award or award, or terminate a contract if a bidder commits or has committed ethical violations, which include, but are not limited to:

1. Offering or giving, directly or indirectly, a bribe, fee, commission, compensation, gift, gratuity, or anything of value to any person or entity in an attempt to influence the bidding process;

2. Utilize the services of lobbyists, attorneys, political activists, or consultants to influence or subvert the bidding process;

3. Being considered for, presently being, or becoming debarred, suspended, ineligible, or excluded from contracting with any state or federal entity:

4. Submitting a proposal on behalf of another Party or entity; and

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

5. Collude with any person or entity to influence the bidding process, submit sham proposals, preclude bidding, fix pricing or costs, create an unfair advantage, subvert the proposal, or prejudice the State.

The Bidder shall include this clause in any subcontract entered into for the exclusive purpose of performing this contract.

Bidder shall have an affirmative duty to report any violations of this clause by the Bidder throughout the bidding process, and throughout the term of this contract for the successful Bidder and their subcontractors.

H. DEVIATIONS FROM THE REQUEST FOR PROPOSAL

The requirements contained in the RFP (Sections II thru VI) become a part of the terms and conditions of the contract resulting from this RFP. Any deviations from the RFP in Sections II through VI must be clearly defined by the bidder in its proposal and, if accepted by the State, will become part of the contract. Any specifically defined deviations must not be in conflict with the basic nature of the RFP, requirements, or applicable state or federal laws or statutes. "Deviation", for the purposes of this RFP, means any proposed changes or alterations to either the contractual language or deliverables within the scope of this RFP. The State discourages deviations and reserves the right to reject proposed deviations.

AT&T Response:

AT&T's Response is submitted pursuant to this Response and subject to the terms of the Proposed Contract Documents. The NASPO/WSCA 3 Contract is a customized contract that allows AT&T to offer robust pricing to customers such as the State. The favorable pricing submitted by this Response, assumes that the State will agree to use the NASPO/WSCA 3 Contract in any final, negotiated contract between the parties in connection with an award to AT&T under this RFP. AT&T's Response is conditioned on the State's willingness to agree to the terms and conditions of the Proposed Contract Documents for the provision of the services requested by this RFP to be provided by AT&T. Except as may be specifically clarified by AT&T in this Response, AT&T takes exception to the terms or conditions contained in the RFP that are inconsistent with the Proposed Contract Documents. This exception is taken regardless of whether AT&T has specifically referenced the Proposed Contract Documents in response to any individual provision in the RFP. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

I. SUBMISSION OF PROPOSALS

Bidders should submit one proposal marked on the first page: "ORIGINAL". If multiple proposals are submitted, the State will retain one copy marked "ORIGINAL" and destroy the other copies. The Bidder is solely responsible for any variance between the copies submitted. Proposal responses should include the completed Form A, "Bidder Proposal Point of Contact". Proposals must reference the RFP number and be sent to the specified address. Please note that the address label should appear as specified in Section I B. on the face of each container or bidder's proposal response packet. If a recipient phone number is required for delivery purposes, 402-471-6500 should be used. The RFP number should be included in all correspondence. The State will not furnish packaging and sealing materials. It is the bidder's responsibility to ensure the RFP is received in a sealed envelope or container and submitted by the date and time indicated in the Schedule of Events. Sealed proposals must be received in the State Purchasing Bureau by the date and time of the proposal opening per the Schedule of Events. No late proposals will be accepted.

The Request for Proposal form must be manually signed in an indelible manner and returned by the proposal opening date and time along with the bidder's Request for Proposal along with any other requirements as stated in the Request for Proposal document in order for the bidder's Request for Proposal response to be evaluated.

It is the responsibility of the bidder to check the website for all information relevant to this Request for Proposal to include addenda and/or amendments issued prior to the opening date. Website address is as follows:
http://das.nebraska.gov/materiel/purchasing.html.

Emphasis should be concentrated on conformance to the RFP instructions, responsiveness to requirements, completeness, and clarity of content. If the bidder's proposal is presented in such a fashion that makes evaluation difficult or overly time consuming the State reserves the right to reject the proposal as non-conforming.

By signing the "Request for Proposal for Contractual Services" form, the bidder guarantees compliance with the provisions stated in this RFP.

AT&T's Clarification:

AT&T agrees as and to the extent responded by AT&T in its Response to this RFP.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

The State shall not incur any liability for any costs incurred by bidders in replying to this RFP, in the demonstrations and/or oral presentations, or in any other activity related to bidding on this RFP.

The Technical and Cost Proposals should be packaged separately (loose-leaf binders are preferred) on standard 8 ½" by 11" paper, except that charts, diagrams and the like may be on fold-outs which, when folded, fit into the 8 ½" by 11" format. Pages may be consecutively numbered for the entire proposal, or may be numbered consecutively within sections. Figures and tables should be numbered and referenced in the text by that number. They should be placed as close as possible to the referencing text. The Technical Proposal should not contain any reference to dollar amounts. However, information such as data concerning labor hours and categories, materials, subcontracts and so forth, shall be considered in the Technical Proposal so that the bidder's understanding of the scope of work may be evaluated. The Technical Proposal shall disclose the bidder's technical approach in as much detail as possible, including, but not limited to, the information required by the Technical Proposal instructions.

AT&T Response:

AT&T has read and understands.

J. PROPOSAL PREPARATION COSTS

The State shall not incur any liability for any costs incurred by Bidders in replying to this RFP, including any activity related to bidding on this RFP.

AT&T Response:

AT&T has read and understands.

K. FAILURE TO COMPLY WITH REQUEST FOR PROPOSAL

Violation of the terms and conditions contained in this RFP or any resultant contract, at any time before or after the award, shall be grounds for action by the State which may include, but is not limited to, the following:

1. Rejection of a bidder's proposal;
2. Withdrawal of the Intent to Award;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

3. Withdrawal of the Award;
4. Negative Vendor Performance Report(s)
5. Termination of the resulting contract;
6. Legal action; and
7. Suspension of the bidder from further bidding with the State for the period of time relative to the seriousness of the violation, such period to be within the sole discretion of the State.

AT&T Response:

AT&T's Response is submitted pursuant to this Response and subject to the terms and conditions of the Proposed Contract Documents. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it.

L. PROPOSAL CORRECTIONS

A bidder may correct a mistake in a proposal prior to the time of opening by giving written notice to the State of intent to withdraw the proposal for modification or to withdraw the proposal completely. Changing a proposal after opening may be permitted if the change is made to correct a minor error that does not affect price, quantity, quality, delivery, or contractual conditions. In case of a mathematical error in extension of price, unit price shall govern.

AT&T Response:

AT&T has read and understands.

M. LATE PROPOSALS

Proposals received after the time and date of the proposal opening will be considered late proposals. Late proposals will be returned unopened, if requested by the bidder and at bidder's expense. The State is not responsible for proposals that are late or lost regardless of cause or fault.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Response:

AT&T has read and understands.

N. PROPOSAL OPENING

The opening of proposals will be public and the bidders will be announced. Proposals **WILL NOT** be available for viewing by those present at the proposal opening. Proposals will be posted to the State Purchasing Bureau website once an Intent to Award has been posted to the website. Information identified as proprietary by the submitting bidder, in accordance with the RFP and state statute, will not be posted. If the state determines submitted information should not be withheld, in accordance with the Public Records Act, or if ordered to release any withheld information, said information may then be released. The submitting contractor will be notified of the release and it shall be the obligation of the submitting bidder to take further action, if it believes the information should not be released. (See RFP signature page for further details) Bidders may contact the State to schedule an appointment for viewing proposals after the Intent to Award has been posted to the website. Once proposals are opened, they become the property of the State of Nebraska and will not be returned.

AT&T's Clarification:

AT&T agrees that the physical response materials become the property of the State. However, any intellectual property of AT&T, AT&T manufacturers or other third parties included in AT&T's Response will remain the property of the respective owner and no title shall transfer by disclosure of such intellectual property as part of AT&T's Response. AT&T further agrees that the State may use its RFP Response as needed in connection with this RFP and the analysis of the AT&T Proposal; provided that AT&T's Proposal may not be shared with third party vendors competing for this RFP and that the State will protect AT&T's Proposal as a confidential document under the terms of applicable open records policies and laws.

O. REQUEST FOR PROPOSAL/PROPOSAL REQUIREMENTS

The proposals will first be examined to determine if all requirements listed below have been addressed and whether further evaluation is warranted. Proposals not meeting the requirements may be rejected as non-responsive. The requirements are:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

1. Original Request for Proposal for Contractual Services form signed using an indelible method;
2. Clarity and responsiveness of the proposal;
3. Completed Corporate Overview;
4. Completed Sections II through VI;
5. Completed Technical Approach; and
6. Completed State Cost Proposal Template.

AT&T Response:

AT&T has read and understands.

P. EVALUATION COMMITTEE

Proposals are evaluated by members of an Evaluation Committee(s). The Evaluation Committee(s) will consist of individuals selected at the discretion of the State. Names of the members of the Evaluation Committee(s) will not be published prior to the intent to award.

Any contact, attempted contact, or attempt to influence an evaluator that is involved with this RFP may result in the rejection of this proposal and further administrative actions.

AT&T Response:

AT&T has read and understands.

Q. EVALUATION OF PROPOSALS

All proposals that are responsive to the RFP will be evaluated. Each evaluation category will have a maximum point potential. The State will conduct a fair, impartial, and comprehensive evaluation of all proposals in accordance with the criteria set forth below. Areas that will be addressed and scored during the evaluation include:

1. Corporate Overview should include but is not limited to:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

a. the ability, capacity, and skill of the bidder to deliver and implement the system or project that meets the requirements of the RFP;

b. the character, integrity, reputation, judgment, experience, and efficiency of the bidder;

c. whether the bidder can perform the contract within the specified timeframe;

d. the quality of vendor performance on prior contracts;

e. such other information that may be secured and that has a bearing on the decision to award the contract;

2. Technical Approach; and,

3. Cost Proposal.

Neb. Rev. Stat. §81-161 allows the quality of performance of previous contracts to be considered when evaluating responses to competitively bid RFPs in determining the lowest responsible bidder. Information obtained from any Vendor Performance Report (See Terms & Conditions, Section H) may be used in evaluating responses to RFPs for goods and services to determine the best value for the State.

Neb. Rev. Stat. §73-107 allows for a preference for a resident disabled veteran or business located in a designated enterprise zone. When a state contract is to be awarded to the lowest responsible bidder, a resident disabled veteran or a business located in a designated enterprise zone under the Enterprise Zone Act shall be allowed a preference over any other resident or nonresident bidder, if all other factors are equal.

Resident disabled veterans means any person (a) who resides in the State of Nebraska, who served in the United States Armed Forces, including any reserve component or the National Guard, who was discharged or otherwise separated with a characterization of honorable or general (under honorable conditions), and who possesses a disability rating letter issued by the United States Department of Veterans Affairs establishing a service-connected disability or a disability determination from the United States Department of Defense and (b)(i) who owns and controls a business or, in the case of a publicly owned business, more than fifty percent of the stock is owned by one or more persons described in subdivision (a) of this subsection and (ii) the management and daily business operations of the business are controlled by one or more persons described in subdivision(a) of this subsection. Any contract entered into without compliance with this section shall be null and void.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Therefore, if a resident disabled veteran or business located in a designated enterprise zone submits a proposal in accordance with Neb. Rev. Stat. §73-107 and has so indicated on the RFP cover page under "Bidder must complete the following" requesting priority/preference to be considered in the award of this contract, the following will need to be submitted by the bidder within ten (10) business days of request:

1. Documentation from the United States Armed Forces confirming service;
2. Documentation of discharge or otherwise separated characterization of honorable or general (under honorable conditions);
3. Disability rating letter issued by the United States Department of Veterans Affairs establishing a service- connected disability or a disability determination from the United States Department of Defense; and
4. Documentation which shows ownership and control of a business or, in the case of a publicly owned business, more than fifty percent of the stock is owned by one or more persons described in subdivision (a) of this subsection; and the management and daily business operations of the business are controlled by one or more persons described in subdivision (a) of this subsection.

Failure to submit the requested documentation within ten (10) business days of notice will disqualify the bidder from consideration of the preference.

Evaluation criteria will be released with the RFP.

AT&T Response:

AT&T has read and understands.

R. COST CLARIFICATION

The State reserves the right to review all aspects of cost for reasonableness and to request clarification of any proposal where the cost component shows significant and unsupported deviation from industry standards or in areas where detailed pricing is required.

AT&T Response:

AT&T has read and understands.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

S. ORAL INTERVIEWS/PRESENTATIONS AND/OR DEMONSTRATIONS

The State may determine after the completion of the Technical and Cost Proposal evaluation that oral interviews/presentations and/or demonstrations are required. Every bidder may not be given an opportunity to interview/present and/or give demonstrations; the State reserves the right, in its discretion, to select only the top scoring bidders to present/give oral interviews. The scores from the oral interviews/presentations and/or demonstrations will be added to the scores from the Technical and Cost Proposals. The presentation process will allow the bidders to demonstrate their proposal offering, explaining and/or clarifying any unusual or significant elements related to their proposals. Bidder's key personnel, identified in their proposal, may be requested to participate in a structured interview to determine their understanding of the requirements of this proposal, their authority and reporting relationships within their firm, and their management style and philosophy. Only representatives of the State and the presenting bidder will be permitted to attend the oral interviews/presentations and/or demonstrations. A written copy or summary of the presentation, and demonstrative information (such as briefing charts, et cetera) may be offered by the bidder, but the State reserves the right to refuse or not consider the offered materials. Bidders shall not be allowed to alter or amend their proposals.

Once the oral interviews/presentations and/or demonstrations have been completed, the State reserves the right to make an award without any further discussion with the bidders regarding the proposals received.

Any cost incidental to the oral interviews/presentations and/or demonstrations shall be borne entirely by the bidder and will not be compensated by the State.

AT&T Response:

AT&T has read and understands.

T. BEST AND FINAL OFFER

If best and final offers (BAFO) are requested by the State and submitted by the bidder, they will be evaluated (using the stated BAFO criteria), scored, and ranked by the Evaluation Committee. The State reserves the right to conduct more than one Best and Final Offer. The award will then be granted to the highest scoring bidder. However, a

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

bidder should provide its best offer in its original proposal. Bidders should not expect that the State will request a best and final offer.

AT&T Response:

AT&T has read and understands.

U. REFERENCE AND CREDIT CHECKS

The State reserves the right to conduct and consider reference and credit checks. The State reserves the right to use third parties to conduct reference and credit checks. By submitting a proposal in response to this RFP, the bidder grants to the State the right to contact or arrange a visit in person with any or all of the bidder's clients. Reference and credit checks may be grounds to reject a proposal, withdraw an intent to award, or rescind the award of a contract.

AT&T Response:

AT&T has read and understands.

V. AWARD

The State reserves the right to evaluate proposals and award contracts in a manner utilizing criteria selected at the State's discretion and in the State's best interest. After evaluation of the proposals, or at any point in the RFP process, the State of Nebraska may take one or more of the following actions:

1. Amend the RFP;
2. Extend the time of or establish a new proposal opening time;
3. Waive deviations or errors in the State's RFP process and in bidder proposals that are not material, do not compromise the RFP process or a bidder's proposal, and do not improve a bidder's competitive position;
4. Accept or reject a portion of or all of a proposal;
5. Accept or reject all proposals;
6. Withdraw the RFP;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

7. Elect to rebid the RFP;

8. Award single lines or multiple lines to one or more bidder's; or,

9. Award one or more all-inclusive contracts.

AT&T Response:

AT&T takes exception to the waiver of "*deviations or errors*" portion of this provision as used here and throughout this RFP to the extent that it implies AT&T waives rights to protest the award decision. To that end, AT&T reserves all protest rights afforded bidders/respondents participating in the State's contracting process.

AT&T Response:

The information and pricing submitted with this RFP is in response to the State's entire bid and may be subject to change on account of partial acceptance by the State.

The RFP does not commit the State to award a contract. Once intent to award decision has been determined, it will be posted to the Internet at: http://das.nebraska.gov/materiel/purchasing.html

Any protests must be filed by a bidder within ten (10) business days after the intent to award decision is posted to the Internet. Grievance and protest procedure is available on the Internet at: http://das.nebraska.gov/materiel/purchasing.html

AT&T Response:

AT&T has read and understands.

W. ALTERNATE/EQUIVALENT PROPOSALS

Bidder may offer proposals which are at variance from the express specifications of the RFP. The State reserves the right to consider and accept such proposals if, in the judgment of the Materiel Administrator, the proposal will result in goods and/or services equivalent to or better than those which would be supplied in the original proposal specifications. Bidder must indicate on the RFP the manufacturer's name, number and shall submit with their proposal, sketches, descriptive literature and/or complete specifications. Reference to literature submitted with a previous proposal will not satisfy this provision. Proposals which do not comply with these requirements are subject to rejection. In the absence of any stated deviation or exception, the proposal

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

will be accepted as in strict compliance with all terms, conditions and specification, and the Bidder shall be held liable therefore.

AT&T Response:

AT&T has read and understands.

X. LUMP SUM OR "ALL OR NONE" PROPOSALS

The State reserves the right to purchase item-by-item, by groups or as a total when the State may benefit by so doing. Bidders may submit a proposal on an "all or none" or "lump sum" basis, but should also submit a proposal on an item-by-item basis. The term "all or none" means a conditional proposal which requires the purchase of all items on which proposals are offered and Bidder declines to accept award on individual items; a "lump sum" proposal is one in which the Bidder offers a lower price than the sum of the individual proposals if all items are purchased, but agrees to deliver individual items at the prices quoted.

AT&T Response:

The information and pricing submitted with this RFP is in response to the State's entire bid and may be subject to change on account of partial acceptance by the State.

Y. EMAIL SUBMISSIONS

SPB will not accept proposals by email, electronic, voice, or telephone proposals except for one-time purchases under $50,000.00.

AT&T Response:

AT&T has read and understands.

Z. REJECTION OF PROPOSALS

The State reserves the right to reject any or all proposals, wholly or in part, in the best interest of the State.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

AT&T Response:

The information and pricing submitted with this RFP is in response to the State's entire bid and may be subject to change on account of partial acceptance by the State.

AA. RESIDENT BIDDER

Pursuant to Neb. Rev. Stat. §§ 73-101.01 through 73-101.02, a Resident Bidder shall be allowed a preference against a Non-resident Bidder from a state which gives or requires a preference to Bidders from that state. The preference shall be equal to the preference given or required by the state of the Nonresident Bidders. Where the lowest responsible bid from a resident Bidder is equal in all respects to one from a nonresident Bidder from a state which has no preference law, the resident Bidder shall be awarded the contract. The provision of this preference shall not apply to any contract for any project upon which federal funds would be withheld because of the provisions of this preference.

AT&T Response:

AT&T has read and understands.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

II. TERMS AND CONDITIONS

AT&T Response:

Notwithstanding anything contained in this RFP to the contrary, AT&T will provide each of the products and services being requested pursuant to the terms and conditions contained in the Proposed Contract Documents and this Response.

The terms and conditions of the Proposed Contract Documents are incorporated herein by reference as part of this proposal and as though set forth in full herein. The products and services proposed hereunder shall be provided solely pursuant to the rates, charges, terms and conditions (including Service Level Agreements) contained in Proposed Contract Documents. Except as may be specifically clarified by AT&T in this Response, AT&T takes exception to any terms or conditions contained in the RFP that are inconsistent with the Proposed Contract Documents. Please note that references to specific Sections within the Proposed Contract Documents are provided solely as a courtesy to assist the State in its review; depending on the issue presented, other provisions within the Proposed Contract Documents may be applicable to fully describe the Parties' rights.

The NASPO/WSCA 3 Contract is a customized contract that allows AT&T to offer robust pricing to customers such as the State. The favorable pricing submitted by this Response, assumes that the State will agree to use the NASPO/WSCA 3 Contract in any final, negotiated contract between the parties in connection with an award to AT&T under this RFP. AT&T's Response is conditioned on the State's willingness to agree to the terms and conditions of the Proposed Contract Documents for the provision of the services requested by this RFP to be provided by AT&T. Except as may be specifically clarified by AT&T in this Response, AT&T takes exception to the terms or conditions contained in the RFP that are inconsistent with the Proposed Contract Documents. This exception is taken regardless of whether AT&T has specifically referenced the Proposed Contract Documents in response to any individual provision in the RFP. Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer.

The AT&T NASPO/WSCA Master Agreement along with Nebraska PA, is currently scheduled to expire on December 31, 2020; therefore, proposed services under this Response for additional years are contingent on AT&T being selected by NASPO/WSCA as one of its vendors on a going forward basis. If so selected by NASPO/WSCA, AT&T will migrate the State to rates, terms and conditions consistent with the new NASPO/WSCA

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

agreement and the new related Participating Addendum for the remaining term of the final agreement between the parties. Revised documentation may be required to transition the State to the new NASPO/WSCA agreement. In the event material changes between the current and future NASPO/WSCA serving arrangements exist, the State may terminate the applicable AT&T Service with no penalty upon the expiration of the existing NASPO/WSCA Master.

Should AT&T be selected as your vendor under this RFP, AT&T will work cooperatively with the State to finalize and/or clarify any contractual provisions required for compliance with the RFP and AT&T's Response to it, and to expedite any purchases made pursuant to this AT&T offer.

Bidders should complete Sections II through VI as part of their proposal. Bidder is expected to read the Terms and Conditions and should initial either accept, reject, or reject and provide alternative language for each clause. The bidder should also provide an explanation of why the bidder rejected the clause or rejected the clause and provided alternate language. By signing the RFP, bidder is agreeing to be legally bound by all the accepted terms and conditions, and any proposed alternative terms and conditions submitted with the proposal. The State reserves the right to negotiate rejected or proposed alternative language. If the State and bidder fail to agree on the final Terms and Conditions, the State reserves the right to reject the proposal. The State of Nebraska is soliciting proposals in response to this RFP. The State of Nebraska reserves the right to reject proposals that attempt to substitute the bidder's commercial contracts and/or documents for this RFP.

The bidder's should submit with their proposal any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The State will not consider incorporation of any document not submitted with the bidder's proposal as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated as addendums if agreed to by the Parties.

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:

1. If only one Party has a particular clause then that clause shall control;
2. If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

3. If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The contract resulting from this RFP shall incorporate the following documents:

1. Request for Proposal and Addenda;
2. Amendments to the RFP;
3. Questions and Answers;
4. Bidder's proposal (RFP and properly submitted documents);
5. The executed Contract and Addendum One to Contract, if applicable; and,
6. Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

Unless otherwise specifically stated in a future contract amendment, in case of any conflict between the incorporated documents, the documents shall govern in the following order of preference with number one (1) receiving preference over all other documents and with each lower numbered document having preference over any higher numbered document: 1) Amendment to the executed Contract with the most recent dated amendment having the highest priority, 2) executed Contract and any attached Addenda, 3) Amendments to RFP and any Questions and Answers, 4) the original RFP document and any Addenda, and 5) the Bidder's submitted Proposal.

Any ambiguity or conflict in the contract discovered after its execution, not otherwise addressed herein, shall be resolved in accordance with the rules of contract interpretation as established in the State of Nebraska.

AT&T Response:

Notwithstanding anything contained in this RFP to the contrary, AT&T's Response is submitted pursuant to this Response and subject to the terms and conditions of the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Proposed Contract Documents. The NASPO/WSCA 3 Contract is a customized contract that allows AT&T to offer robust pricing to customers such as the State. The favorable pricing submitted by this Response, assumes that the District will agree to use the NASPO/WSCA 3 Contract in any final, negotiated contract between the parties in connection with an award to AT&T under this RFP. AT&T's Response is conditioned on the State's willingness to agree to the terms and conditions of the Proposed Contract Documents for the provision of the services requested by this RFP to be provided by AT&T.

B. NOTIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Bidder and State shall identify the contract manager who shall serve as the point of contact for the executed contract.

Communications regarding the executed contract shall be in writing and shall be deemed to have been given if delivered personally or mailed, by U.S. Mail, postage prepaid, return receipt requested, to the parties at their respective addresses set forth below, or at such other addresses as may be specified in writing by either of the parties. All notices, requests, or communications shall be deemed effective upon personal delivery or five (5) calendar days following deposit in the mail.

Either party may change its address for notification purposes by giving notice of the change, and setting forth the new address and an effective date.

AT&T Response:

AT&T's Response is submitted pursuant to this Response and subject to the terms and conditions of the Proposed Contract Documents. All terms and conditions relating to notice shall be as set out in said Proposed Contract Documents.

C. NOTICE (POC)

The State reserves the right to appoint a Buyer's Representative to manage [or assist the Buyer in managing] the contract on behalf of the State. The Buyer's Representative will be appointed in writing, and the appointment document will specify the extent of the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Buyer's Representative authority and responsibilities. If a Buyer's Representative is appointed, the Bidder will be provided a copy of the appointment document, and is expected to cooperate accordingly with the Buyer's Representative. The Buyer's Representative has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

D. GOVERNING LAW (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must be brought in the State of Nebraska per state law; (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity, limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

The Parties must comply with all applicable local, state and federal laws, ordinances, rules, orders, and regulations.

AT&T Response:

AT&T shall comply with all laws and regulations applicable to AT&T. AT&T will provide the services as outlined in its proposal and resulting contract documents in a manner mutually agreed by the parties. Please see Section 44.2 ("Governing Law; Jurisdiction") of the AT&T NASPO/WSCA Master Agreement.

E. BEGINNING OF WORK

The bidder shall not commence any billable work until a valid contract has been fully executed by the State and the successful Bidder. The Bidder will be notified in writing when work may begin.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

F. AMENDMENT

This Contract may be amended in writing, within scope, upon the agreement of both parties.

G. CHANGE ORDERS OR SUBSTITUTIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T's proposal hereunder is a direct reflection of the scope of work as presented here, as of the date of submission. Changes/modifications made after submission will require mutual agreement/adjustment to the final configuration, subsequent pricing and implementation schedule. For the price quoted AT&T will provide the equipment and services listed.

The State and the Contractor, upon the written agreement, may make changes to the contract within the general scope of the RFP. Changes may involve specifications, the quantity of work, or such other items as the State may find necessary or desirable. Corrections of any deliverable, service, or work required pursuant to the contract shall not be deemed a change. The Contractor may not claim forfeiture of the contract by reasons of such changes.

The Contractor shall prepare a written description of the work required due to the change and an itemized cost sheet for the change. Changes in work and the amount of compensation to be paid to the Contractor shall be determined in accordance with applicable unit prices if any, a pro-rated value, or through negotiations. The State shall not incur a price increase for changes that should have been included in the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Contractor's proposal, were foreseeable, or result from difficulties with or failure of the Contractor's proposal or performance.

No change shall be implemented by the Contractor until approved by the State, and the Contract is amended to reflect the change and associated costs, if any. If there is a dispute regarding the cost, but both parties agree that immediate implementation is necessary, the change may be implemented, and cost negotiations may continue with both Parties retaining all remedies under the contract and law.

In the event any product is discontinued or replaced upon mutual consent during the contract period or prior to delivery, the State reserves the right to amend the contract or purchase order to include the alternate product at the same price.

*****Contractor will not substitute any item that has been awarded without prior written approval of SPB*****

H. VENDOR PERFORMANCE REPORT(S)

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T will endeavor to meet all mutually agreed contract obligations; however, AT&T shall not be liable for any problems caused by force majeure, delays due to any fault of the State and/or any contractor or subcontractor employed by the State, manufacturer (to include Equipment which may be on "back order") or network delays, or for problems resulting from causes beyond the reasonable control of AT&T. AT&T's proposal is submitted subject to the remedy and termination provisions of the Proposed Contract Documents.

The State may document any instance(s) of products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or RFP specifications. The State Purchasing Bureau may contact the Vendor regarding any such

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

report. Vendor performance report(s) will become a part of the permanent record of the Vendor.

I. NOTICE OF POTENTIAL CONTRACTOR BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 4 ("Cancellation Notice"), Section 21 ("Default: Remedies") and Section 23 ("Limited Liability") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04,

If Contractor breaches the contract or anticipates breaching the contract, the Contractor shall immediately give written notice to the State. The notice shall explain the breach or potential breach, a proposed cure, and may include a request for a waiver of the breach if so desired. The State may, in its discretion, temporarily or permanently waive the breach. By granting a waiver, the State does not forfeit any rights or remedies to which the State is entitled by law or equity, or pursuant to the provisions of the contract. Failure to give immediate notice, however, may be grounds for denial of any request for a waiver of a breach.

J. BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 4 ("Cancellation Notice"), Section 21 ("Default: Remedies") and Section 23 ("Limited Liability") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Addendum Contract 55001 04.

Either Party may terminate the contract, in whole or in part, if the other Party breaches its duty to perform its obligations under the contract in a timely and proper manner. Termination requires written notice of default and a thirty (30) calendar day (or longer at the non-breaching Party's discretion considering the gravity and nature of the default) cure period. Said notice shall be delivered by Certified Mail, Return Receipt Requested, or in person with proof of delivery. Allowing time to cure a failure or breach of contract does not waive the right to immediately terminate the contract for the same or different contract breach which may occur at a different time. In case of default of the Contractor, the State may contract the service from other sources and hold the Contractor responsible for any excess cost occasioned thereby. OR In case of breach by the Contractor, the State may, without unreasonable delay, make a good faith effort to make a reasonable purchase or contract to purchased goods in substitution of those due from the contractor. The State may recover from the Contractor as damages the difference between the costs of covering the breach. Notwithstanding any clause to the contrary, the State may also recover the contract price together with any incidental or consequential damages defined in UCC Section 2- 715, but less expenses saved in consequence of Contractor's breach.

The State's failure to make payment shall not be a breach, and the Contractor shall retain all available statutory remedies and protections.

K. NON-WAIVER OF BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 4 ("Cancellation Notice"), Section 21 ("Default: Remedies"), Section 23 ("Limited Liability") and Section 28 ("Waiver of Breach") of the NASPO/WSCA Master Agreement.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

The acceptance of late performance with or without objection or reservation by a Party shall not waive any rights of the Party nor constitute a waiver of the requirement of timely performance of any obligations remaining to be performed.

L. SEVERABILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Please see Section 29 ("Severability"), of the NASPO/WSCA Master Agreement?

If any term or condition of the contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and conditions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the provision held to be invalid or illegal.

M. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Please see Section 25 ("Indemnification") of the NASPO/WSCA Master Agreement.

1. GENERAL

The Contractor agrees to defend, indemnify, and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials ("the indemnified parties") from and against any and all third party claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and expenses, settlement costs, and attorney fees and expenses ("the claims"), sustained or asserted against the State for personal injury, death, or property loss or damage, arising out of, resulting from,

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

or attributable to the willful misconduct, negligence, error, or omission of the Contractor, its employees, subcontractors, consultants, representatives, and agents, resulting from this contract, except to the extent such Contractor liability is attenuated by any action of the State which directly and proximately contributed to the claims.

2. **INTELLECTUAL PROPERTY (Optional)**

The Contractor agrees it will, at its sole cost and expense, defend, indemnify, and hold harmless the indemnified parties from and against any and all claims, to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of any patent, copyright, trade secret, trademark, or confidential information of any third party by the Contractor or its employees, subcontractors, consultants, representatives, and agents; provided, however, the State gives the Contractor prompt notice in writing of the claim. The Contractor may not settle any infringement claim that will affect the State's use of the Licensed Software without the State's prior written consent, which consent may be withheld for any reason.

If a judgment or settlement is obtained or reasonably anticipated against the State's use of any intellectual property for which the Contractor has indemnified the State, the Contractor shall, at the Contractor's sole cost and expense, promptly modify the item or items which were determined to be infringing, acquire a license or licenses on the State's behalf to provide the necessary rights to the State to eliminate the infringement, or provide the State with a non-infringing substitute that provides the State the same functionality. At the State's election, the actual or anticipated judgment may be treated as a breach of warranty by the Contractor, and the State may receive the remedies provided under this RFP.

3. **PERSONNEL**

The Contractor shall, at its expense, indemnify and hold harmless the indemnified parties from and against any claim with respect to withholding taxes, worker's compensation, employee benefits, or any other claim, demand, liability, damage, or loss of any nature relating to any of the personnel, including subcontractor's and their employees, provided by the Contractor.

4. **SELF-INSURANCE**

The State of Nebraska is self-insured for any loss and purchases excess insurance coverage pursuant to Neb. Rev. Stat. § 81-8,239.01 (Reissue 2008). If there is a presumed loss under the provisions of this agreement, Contractor may file a claim

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

with the Office of Risk Management pursuant to Neb. Rev. Stat. §§ 81-8,829 – 81-8,306 for review by the State Claims Board. The State retains all rights and immunities under the State Miscellaneous (Section 81-8,294), Tort (Section 81-8,209), and Contract Claim Acts (Section 81-8,302), as outlined in Neb. Rev. Stat. § 81-8,209 et seq. and under any other provisions of law and accepts liability under this agreement to the extent provided by law.

5. The Parties acknowledge that Attorney General for the State of Nebraska is required by statute to represent the legal interests of the State, and that any provision of this indemnity clause is subject to the statutory authority of the Attorney General.

AT&T Response:

Please see Section 26 ("Insurance Schedule") of the NASPO/WSCA Master Agreement.

N. ATTORNEY'S FEES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T cannot agree to this section as written. For clarification, AT&T does not agree to pay attorney's fees and expenses incurred by the State.

In the event of any litigation, appeal, or other legal action to enforce any provision of the contract, the Parties agree to pay all expenses of such action, as permitted by law and if ordered by the court, including attorney's fees and costs, if the other Party prevails.

O. ASSIGNMENT, SALE, OR MERGER

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 30 ("Assignment/Delegation") of the NASPO/WSCA Master Agreement.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Either Party may assign the contract upon mutual written agreement of the other Party. Such agreement shall not be unreasonably withheld.

The Contractor retains the right to enter into a sale, merger, acquisition, internal reorganization, or similar transaction involving Contractor's business. Contractor agrees to cooperate with the State in executing amendments to the contract to allow for the transaction. If a third party or entity is involved in the transaction, the Contractor will remain responsible for performance of the contract until such time as the person or entity involved in the transaction agrees in writing to be contractually bound by this contract and perform all obligations of the contract.

P. CONTRACTING WITH OTHER NEBRASKA POLITICAL SUB-DIVISIONS OF THE STATE OR ANOTHER STATE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 42 ("Political Subdivision Participation") of the NASPO/WSCA Master Agreement.

The Contractor may, but shall not be required to, allow agencies, as defined in Neb. Rev. Stat. §81-145, to use this contract. The terms and conditions, including price, of the contract may not be amended. The State shall not be contractually obligated or liable for any contract entered into pursuant to this clause. A listing of Nebraska political subdivisions may be found at the website of the Nebraska Auditor of Public Accounts.

The Contractor may, but shall not be required to, allow other states, agencies or divisions of other states, or political subdivisions of other states to use this contract. The terms and conditions, including price, of this contract shall apply to any such contract, but may be amended upon mutual consent of the Parties. The State of Nebraska shall not be contractually or otherwise obligated or liable under any contract entered into pursuant to this clause. The State shall be notified if a contract is executed based upon this contract.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Q. FORCE MAJEURE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 24 ("Force Majeure") of the NASPO/WSCA Master Agreement.

Neither Party shall be liable for any costs or damages, or for default resulting from its inability to perform any of its obligations under the contract due to a natural or manmade event outside the control and not the fault of the affected Party ("Force Majeure Event"). The Party so affected shall immediately make a written request for relief to the other Party, and shall have the burden of proof to justify the request. The other Party may grant the relief requested; relief may not be unreasonably withheld. Labor disputes with the impacted Party's own employees will not be considered a Force Majeure Event.

R. CONFIDENTIALITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 34("Confidentiality") of the NASPO/WSCA Master Agreement.

All materials and information provided by the Parties or acquired by a Party on behalf of the other Party shall be regarded as confidential information. All materials and information provided or acquired shall be handled in accordance with federal and state law, and ethical standards. Should said confidentiality be breached by a Party, the Party shall notify the other Party immediately of said breach and take immediate corrective action.

It is incumbent upon the Parties to inform their officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1), which is made applicable by 5 U.S.C. 552a (m)(1), provides that any officer or employee, who by virtue of his/her employment or official position has possession of or access to agency records which contain individually identifiable

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

S. EARLY TERMINATION

Accept (initial)	Reject (initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 4 ("Cancellation Notice"), Section 21 ("Default: Remedies") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

The contract may be terminated as follows:

1. The State and the Contractor, by mutual written agreement, may terminate the contract at anytime.

2. The State, in its sole discretion, may terminate the contract for any reason upon thirty (30) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided.

3. The State may terminate the contract immediately for the following reasons:

   a. if directed to do so by statute;

   b. Contractor has made an assignment for the benefit of creditors, has admitted in writing its inability to pay debts as they mature, or has ceased operating in the normal course of business;

   c. a trustee or receiver of the Contractor or of any substantial part of the Contractor's assets has been appointed by a court;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

d. fraud, misappropriation, embezzlement, malfeasance, misfeasance, or illegal conduct pertaining to performance under the contract by its Contractor, its employees, officers, directors, or shareholders;

e. an involuntary proceeding has been commenced by any Party against the Contractor under any one of the chapters of Title 11 of the United States Code and (i) the proceeding has been pending for at least sixty (60) calendar days; or (ii) the Contractor has consented, either expressly or by operation of law, to the entry of an order for relief; or (iii) the Contractor has been decreed or adjudged a debtor;

f. a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;

g. Contractor intentionally discloses confidential information;

h. Contractor has or announces it will discontinue support of the deliverable; and,

i. In the event funding is no longer available.

T. CONTRACT CLOSEOUT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 21 ("Default: Remedies") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

Upon contract closeout for any reason the Contractor shall within 30 days, unless stated otherwise herein:

1. Transfer all completed or partially completed deliverables to the State;

2. Transfer ownership and title to all completed or partially completed deliverables to the State;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

3. Return to the State all information and data, unless the Contractor is permitted to keep the information or data by contract or rule of law. Contractor may retain one copy of any information or data as required to comply with applicable work product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures;

4. Cooperate with any successor Contactor, person or entity in the assumption of any or all of the obligations of this contract;

5. Cooperate with any successor Contactor, person or entity with the transfer of information or data related to this contract;

6. Return or vacate any state owned real or personal property; and,

7. Return all data in a mutually acceptable format and manner.

Nothing in this Section should be construed to require the Contractor to surrender intellectual property, real or personal property, or information or data owned by the Contractor for which the State has no legal claim.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

III. CONTRACTOR DUTIES

A. INDEPENDENT CONTRACTOR /OBLIGATIONS

Accept (initial)	Reject (initial)	Reject & Provide Alternative within RFP Response (initial)	NOTES/COMMENTS:
			As to Independent Contractor - Please see Section 41 ("Independent Contractor"), of the NASPO/WSCA Master Agreement. As to Request for Change of Personnel - AT&T shall employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with the State's operations and use of telecommunications services, to provide and support the State's use of the Services in accordance with the terms of AT&T's response to this RFP. AT&T retains the right to manage and deploy its personnel as appropriate from time to time. If the State requests AT&T to substitute an employee or subcontractor, the State shall provide such requests in writing, explaining in reasonable detail the reason(s) for the removal request. Any such request shall be for lawful reasons. AT&T will work with the State to reach a solution geared to providing

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
		Services in compliance with contracted standards. As to AT&T's Compliance with the stated labor laws - Please see Section 27 ("Compliance with Legal Obligations"), of the NASPO/WSCA Master Agreement.	

It is agreed that the Contractor is an independent contractor and that nothing contained herein is intended or should be construed as creating or establishing a relationship of employment, agency, or a partnership.

The Contractor is solely responsible for fulfilling the contract. The Contractor or the Contractor's representative shall be the sole point of contact regarding all contractual matters.

The Contractor shall secure, at its own expense, all personnel required to perform the services under the contract. The personnel the Contractor uses to fulfill the contract shall have no contractual or other legal relationship with the State; they shall not be considered employees of the State and shall not be entitled to any compensation, rights or benefits from the State, including but not limited to, tenure rights, medical and hospital care, sick and vacation leave, severance pay, or retirement benefits.

By-name personnel commitments made in the Contractor's proposal shall not be changed without the prior written approval of the State. Replacement of these personnel, if approved by the State, shall be with personnel of equal or greater ability and qualifications.

All personnel assigned by the Contractor to the contract shall be employees of the Contractor or a subcontractor, and shall be fully qualified to perform the work required herein. Personnel employed by the Contractor or a subcontractor to fulfill the terms of the contract shall remain under the sole direction and control of the Contractor or the subcontractor respectively.

With respect to its employees, the Contractor agrees to be solely responsible for the following:

1. Any and all pay, benefits, and employment taxes and/or other payroll withholding;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

2. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;

3. Damages incurred by Contractor's employees within the scope of their duties under the contract;

4. Maintaining Workers' Compensation and health insurance that complies with state and federal law and submitting any reports on such insurance to the extent required by governing law;

5. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,

6. All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination alleged against the Contractor, its officers, agents, or subcontractors or subcontractor's employees)

If the Contractor intends to utilize any subcontractor, the subcontractor's level of effort, tasks, and time allocation should be clearly defined in the contractor's proposal. The Contractor shall agree that it will not utilize any subcontractors not specifically included in its proposal in the performance of the contract without the prior written authorization of the State.

The State reserves the right to require the Contractor to reassign or remove from the project any Contractor or subcontractor employee.

Contractor shall insure that the terms and conditions contained in any contract with a subcontractor does not conflict with the terms and conditions of this contract.

The Contractor shall include a similar provision, for the protection of the State, in the contract with any subcontractor engaged to perform work on this contract.

B. EMPLOYEE WORK ELIGIBILITY STATUS

Accept (initial)	Reject (initial)	Reject & Provide Alternative within RFP Response (initial)	NOTES/COMMENTS:

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of employees physically performing services within the State of Nebraska. A federal immigration verification system means

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of an employee.

If the Contractor is an individual or sole proprietorship, the following applies:

1. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html
2. The completed United States Attestation Form should be submitted with the RFP response.
3. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.
4. The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

C. COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory)

The Contractor shall comply with all applicable local, state, and federal statutes and regulations regarding civil rights laws and equal opportunity employment. The Nebraska Fair Employment Practice Act prohibits Contractors of the State of Nebraska, and their subcontractors, from discriminating against any employee or applicant for employment, with respect to hire, tenure, terms, conditions, compensation, or privileges of employment because of race, color, religion, sex, disability, marital status, or national origin (Neb. Rev. Stat. §48-1101 to 48-1125). The Contractor guarantees compliance with the Nebraska Fair Employment Practice Act, and breach of this provision shall be regarded as a material breach of contract. The Contractor shall insert a similar provision in all Subcontracts for goods and services to be covered by any contract resulting from this RFP.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Response:

AT&T is an Equal Opportunity Employer. Please also see Section 27 ("Compliance with Legal Obligations"), of the NASPO/WSCA Master Agreement.

D. COOPERATION WITH OTHER CONTRACTORS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T will endeavor to work cooperatively with other providers, but will not be responsible for delays due to any fault of the State and/or any contractor or subcontractor employed by the State, or for problems resulting from causes beyond the reasonable control of AT&T.

Contractor may be required to work with or in close proximity to other contractors or individuals that may be working on same or different projects. The Contractor shall agree to cooperate with such other contractors or individuals, and shall not commit or permit any act which may interfere with the performance of work by any other contractor or individual. Contractor is not required to compromise Contractor's intellectual property or proprietary information unless expressly required to do so by this contract.

E. DISCOUNTS

Prices quoted shall be inclusive of ALL trade discounts. Cash discount terms of less than thirty (30) days will not be considered as part of the proposal. Cash discount periods will be computed from the date of receipt of a properly

executed claim voucher or the date of completion of delivery of all items in a satisfactory condition, whichever is later.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

F. PRICES

Prices quoted shall be net, including transportation and delivery charges fully prepaid by the contractor, F.O.B. destination named in the RFP. No additional charges will be allowed for packing, packages, or partial delivery costs. When an arithmetic error has been made in the extended total, the unit price will govern.

AT&T Response:

As to this entire Subsection 7, please see Section 17 ("Delivery"), of the NASPO/WSCA Master Agreement.

All prices, costs, and terms and conditions submitted in the proposal shall remain fixed and valid commencing on the opening date of the proposal until an award is made or the RFP is cancelled.

Cost submitted for Year One, Year Two and Year Three of the initial period are firm for the entire contract period each year and cannot increase. Price escalation of no more than 3% may be allowed for each renewal period.

Any request for an increase must be submitted in writing to the State Purchasing Bureau a minimum of 30 days prior to contract renewal date, and must show cause and be accompanied by supporting documentation. Failure to supply any requested supporting documentation may be ground to reject the requested increase and cancel the contract. The State further reserves the right to reject any proposed price increase(s), cancel the contract and re-bid if determined to be in the best interest of the State. The State will be given full proportionate benefit of any decrease for the term of the contract. No price increases are to be billed to the State without prior written approval by the State Purchasing Bureau.

The State reserves the right to deny any requested price increase. No price increases are to be billed to any State Agencies prior to written amendment of the contract by the parties.

The State will be given full proportionate benefit of any decreases for the term of the contract.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

G. PERMITS, REGULATIONS, LAWS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 27 ("Compliance with Legal Obligations"), of the NASPO/WSCA Master Agreement.

The contract price shall include the cost of all royalties, licenses, permits, and approvals, whether arising from patents, trademarks, copyrights or otherwise, that are in any way involved in the contract. The Contractor shall obtain and pay for all royalties, licenses, and permits, and approvals necessary for the execution of the contract. The Contractor must guarantee that it has the full legal right to the materials, supplies, equipment, software, and other items used to execute this contract.

H. OWNERSHIP OF INFORMATION AND DATA /DELIVERABLES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 31 ("Ownership of Proprietary Information"), of the NASPO/WSCA Master Agreement. AT&T clarifies that only the physical response materials become the State's property. Any other pre-existing or newly-developed intellectual property of AT&T, its suppliers or its third parties, provided in this RFP response or which is used or developed during the project remains the intellectual property of AT&T or its suppliers.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

The State shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or obtained by the Contractor on behalf of the State pursuant to this contract.

The State shall own and hold exclusive title to any deliverable developed as a result of this contract. Contractor shall have no ownership interest or title, and shall not patent, license, or copyright, duplicate, transfer, sell, or exchange, the design, specifications, concept, or deliverable.

I. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 26 ("Insurance Schedule") of the NASPO/WSCA Master Agreement.

The Contractor shall throughout the term of the contract maintain insurance as specified herein and provide the State a current Certificate of Insurance/Acord Form (COI) verifying the coverage. The Contractor shall not commence work on the contract until the insurance is in place. If Contractor subcontracts any portion of the Contract the Contractor must, throughout the term of the contract, either:

1. Provide equivalent insurance for each subcontractor and provide a COI verifying the coverage for the subcontractor;

2. Require each subcontractor to have equivalent insurance and provide written notice to the State that the Contractor has verified that each subcontractor has the required coverage; or,

3. Provide the State with copies of each subcontractor's Certificate of Insurance evidencing the required coverage.

The Contractor shall not allow any subcontractor to commence work until the subcontractor has equivalent insurance. The failure of the State to require a COI, or the failure of the Contractor to provide a COI or require subcontractor insurance shall not limit, relieve, or decrease the liability of the Contractor hereunder.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

In the event that any policy written on a claims-made basis terminates or is canceled during the term of the contract or within one (1) years of termination or expiration of the contract, the contractor shall obtain an extended discovery or reporting period, or a new insurance policy, providing coverage required by this contract for the term of the contract and one (1) years following termination or expiration of the contract.

If by the terms of any insurance a mandatory deductible is required, or if the Contractor elects to increase the mandatory deductible amount, the Contractor shall be responsible for payment of the amount of the deductible in the event of a paid claim.

Notwithstanding any other clause in this Contract, the State may recover up to the liability limits of the insurance policies required herein.

1. WORKERS' COMPENSATION INSURANCE

The Contractor shall take out and maintain during the life of this contract the statutory Workers' Compensation and Employer's Liability Insurance for all of the contactors' employees to be engaged in work on the project under this contract and, in case any such work is sublet, the Contractor shall require the subcontractor similarly to provide Worker's Compensation and Employer's Liability Insurance for all of the subcontractor's employees to be engaged in such work. This policy shall be written to meet the statutory requirements for the state in which the work is to be performed, including Occupational Disease. **The policy shall include a waiver of subrogation in favor of the State. The COI shall contain the mandatory COI subrogation waiver language found hereinafter**. The amounts of such insurance shall not be less than the limits stated hereinafter. For employees working in the State of Nebraska, the policy must be written by an entity authorized by the State of Nebraska Department of Insurance to write Workers' Compensation and Employer's Liability Insurance for Nebraska employees.

2. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE

The Contractor shall take out and maintain during the life of this contract such Commercial General Liability Insurance and Commercial Automobile Liability Insurance as shall protect Contractor and any subcontractor performing work covered by this contract from claims for damages for bodily injury, including death, as well as from claims for property damage, which may arise from operations under this contract, whether such operation be by the Contractor or by any subcontractor or by anyone directly or indirectly employed by either of them, and the amounts of such insurance shall not be less than limits stated hereinafter.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

The Commercial General Liability Insurance shall be written on an **occurrence basis**, and provide Premises/Operations, Products/Completed Operations, Independent Contractors, Personal Injury, and

Contractual Liability coverage. The policy shall include the State, and others as required by the contract documents, as Additional Insured(s). This policy shall be primary, and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory. The COI shall contain the mandatory COI liability waiver language found hereinafter. The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles.

REQUIRED INSURANCE COVERAGE	
COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Medical Payments	$10,000 any one person
Damage to Rented Premises (Fire)	$300,000 each occurrence
Contractual	Included
XCU Liability (Explosion, Collapse, and Underground Damage)	Included
Independent Contractors	Included

If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.

WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K
Statutory Limits- All States	Statutory - State of Nebraska
USL&H Endorsement	Statutory
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$5,000,000 per occurrence
PROFESSIONAL LIABILITY	
Qualification Under Nebraska Excess Fund	
All Other Professional Liability (Errors & Omissions)	$1,000,000 Per Claim / Aggregate

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

COMMERCIAL CRIME	
Crime/Employee Dishonesty Including 3rd Party Fidelity	$1,000,000
CYBER LIABILITY	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	$10,000,000
CONTRACTOR'S POLLUTION LIABILITY	
Each Occurrence/Aggregate Limit	$2,000,000
Includes Non-Owned Disposal Sites	

MANDATORY COI SUBROGATION WAIVER LANGUAGE

"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."

MANDATORY COI LIABILITY WAIVER LANGUAGE

"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory as additionally insured."

3. EVIDENCE OF COVERAGE

The Contractor shall furnish the Contract Manager, with a certificate of insurance coverage complying with the above requirements prior to beginning work at:

Agency: OCIO Purchasing
Attn: Contract Manager
501 South 14th Street
Lincoln, NE 68509

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts and types of coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

Reasonable notice of cancellation of any required insurance policy must be submitted to the contract manager as listed above when issued and a new coverage binder shall be submitted immediately to ensure no break in coverage.

4. DEVIATIONS

The insurance requirements are subject to limited negotiation. Negotiation typically includes, but is not necessarily limited to, the correct type of coverage, necessity for

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Workers' Compensation, and the type of automobile coverage carried by the Contractor.

J. NOTICE OF POTENTIAL CONTRACTOR BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 4 ("Cancellation Notice"), Section 21 ("Default: Remedies") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

If Contractor breaches the contract or anticipates breaching the contract the Contractor shall immediately give written notice to the State. The notice shall explain the breach or potential breach, and may include a request for a waiver of the breach if so desired. The State may, at its discretion, temporarily or permanently waive the breach. By granting a temporary waiver, the State does not forfeit any rights or remedies to which the State is entitled by law or equity, or pursuant to the provisions of the contract. Failure to give immediate notice, however, may be grounds for denial of any request for a waiver of a breach.

K. ANTITRUST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T will work with the State to reach agreement on a mutually acceptable assignment of anti-trust claim provision. AT&T counter proposes and will agree to the following language: "AT&T hereby assigns to the State any and all antitrust claims for overcharges to the extent associated with the volume of products and services provided to the State under any

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			contract resulting from this RFP, when such claims arise under the antitrust laws of the United States, 15 U.S.C. Section 1, et seq. (1973), as amended, and the antitrust laws of the State of Nebraska

The Contractor hereby assigns to the State any and all claims for overcharges as to goods and/or services provided in connection with this contract resulting from antitrust violations which arise under antitrust laws of the United States and the antitrust laws of the State.

L. CONFLICT OF INTEREST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T is not aware of any material conflict of interest. AT&T is publicly owned, and with millions of shareholders, it is impossible for AT&T to determine whether any State employee may be a shareholder in AT&T, Inc. However, the State should make such an inquiry of its own employees, directors, and officers prior to entering into an agreement with AT&T and take the necessary steps to ensure such individuals remain in compliance with these State requirements.

By submitting a proposal, bidder certifies that no relationship exists between the bidder and any person or entity which either is, or gives the appearance of, a conflict of interest related to this Request for Proposal or project.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Bidder further certifies that bidder will not employ any individual known by bidder to have a conflict of interest nor shall bidder take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its contractual obligations hereunder or which creates an actual or appearance of conflict of interest.

If there is an actual or perceived conflict of interest, bidder shall provide with its proposal a full disclosure of the facts describing such actual or perceived conflict of interest and a proposed mitigation plan for consideration. The State will then consider such disclosure and proposed mitigation plan and either approve or reject as part of the overall bid evaluation.

M. STATE PROPERTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T will repair and replace any damage to the State's premises due to the installation effort caused by AT&T or its agents, as promptly as reasonably practicable, returning the site to its pre-installation condition.

The Contractor shall be responsible for the proper care and custody of any State-owned property which is furnished for the Contractor's use during the performance of the contract. The Contractor shall reimburse the State for any loss or damage of such property; normal wear and tear is expected.

N. SITE RULES AND REGULATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			AT&T's Response is submitted under applicable laws and regulations current at the time of contract execution. AT&T shall comply with all laws applicable to AT&T. Changes

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			in laws and regulations may require changes in pricing and performance.

The Contractor shall use its best efforts to ensure that its employees, agents, and subcontractors comply with site rules and regulations while on State premises. If the Contractor must perform on-site work outside of the daily operational hours set forth by the State, it must make arrangements with the State to ensure access to the facility and the equipment has been arranged. No additional payment will be made by the State on the basis of lack of access, unless the State fails to provide access as agreed to in writing between the State and the Contractor.

O. ADVERTISING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor agrees not to refer to the contract award in advertising in such a manner as to state or imply that the company or its goods or services are endorsed or preferred by the State. Any publicity releases pertaining to the project shall not be issued without prior written approval from the State.

P. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory)

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2- 201.html and ensure that products and/or services provided under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Q. DISASTER RECOVERY/BACK UP PLAN

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

The Contractor shall have a disaster recovery and back-up plan, of which a copy should be provided upon request to the State, which includes, but is not limited to equipment, personnel, facilities, and transportation, in order to continue delivery of goods and services as specified under the specifications in the contract in the event of a disaster.

AT&T Response:

Please see AT&T Attachments: Business_Continuity_Handbook.

R. DRUG POLICY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please also refer to Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

Contractor certifies it maintains a drug free work place environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon request by the State.

AT&T Response:

During the hiring process, we collect important information about U.S. job applicants, such as criminal records and employment verification.

Prior to employment, all job applicants must complete the AT&T employment application and paperwork authorizing AT&T or its authorized vendor to conduct required background checks. This includes

- Misdemeanor and felony convictions searches in all counties where the candidate has resided, worked, or attended school during the past seven years

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

(we provide exclusions to required disclosure of criminal convictions in specific states)

- Nationwide criminal database searches
- National Sex Offender Registry checks
- Federal convictions searches in all jurisdictions where the candidate has resided, worked, or attended school during the past seven years
- International criminal background checks for candidates who have lived, worked, or gone to school in another country during the past seven years—if allowable under that country's laws and if the individual was over the age of 18 at the time
- Motor Vehicle Record reports for driving positions and positions requiring a Department of Transportation (DOT) check
- Employment verification for the previous five-year period (seven years for management candidates), and longer for DOT positions, or a DD214 verification if the individual has served in the military during that period

Additional requirements include

- Self-disclosure of criminal convictions (both misdemeanor and felony, including federal and sex offenses)
- A Social Security number (SSN) name and address history trace to identify previous names and addresses associated with the SSN provided by the candidate
- SSN validation against the Death Master Index to make sure that it doesn't belong to a deceased person and that it's valid (it also provides the state of issuance and approximate year of issuance to verify that it was after the candidate' s birthdate)
- Education verification for all applicants claiming to have a degree and, in some instances, verification of hours attended, specific certifications, and/or professional licenses
- For certain positions in Oklahoma, a check of the candidate' s name against the Oklahoma Sex Offender Registry and Marry Rippy Violent Crime Offender Registry
- Substance abuse screening (initial employment offers are conditional upon the results of a drug urinalysis test)

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

- A government security investigation for positions that require Secret, Top Secret, and/or Top Secret SCI Security Clearance and candidate eligibility for access to classified information

Government check lists that we search include

- The List of Specially Designated Nationals and Other Blocked Persons that the U.S. Department of the Treasury, Office of Foreign Assets Control maintains and that lists individuals subject to OFAC trade sanctions (including terrorists, narcotics traffickers, and other blocked persons) with whom dealings by U.S. citizens (in the case of terrorists and certain dealings by non-U.S. citizens) are prohibited: https://www.treasury.gov/ofac/downloads/sdnlist.pdf
- The List of Denied Parties that the U.S. Department of Commerce, Bureau of Industry and Security maintains pursuant to the Export Administration Regulations (EAR) and that lists persons and entities who've been denied export privileges for a certain period for violations of the EAR or other export laws: http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list
- The Entity List that the U.S. Department of Commerce, Bureau of Industry and Security maintains pursuant to the EAR that lists persons and entities deemed to pose a proliferation risk: http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
- The Unverified Parties List that the U.S. Department of Commerce, Bureau of Industry and Security maintains pursuant to the EAR and that lists foreign persons who were parties to a transaction for which BIS couldn't conduct a pre-license check or a post-shipment verification: http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/unverified-list
- The Nonproliferation Lists that the State Department compiles of parties that have been sanctioned under various non-proliferation statutes: http://www.state.gov/t/isn/c15231.htm
- The State Department's Debarred Parties List of parties debarred from participating directly or indirectly in the export of defense articles, including technical data or in the furnishing of defense services for which the International Traffic in Arms Regulations require a license or approval: https://www.pmddtc.state.gov/compliance/debar.html

To provide you with the best service and support, our goal is to hire the best employees.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

S. WARRANTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			All terms and conditions relating to warranties shall be as set forth in the Proposed Contract Documents. While AT&T does not provide any direct warranty, AT&T will pass through to NEM any equipment or software warranties available from its Purchased Equipment suppliers, to the extent that AT&T is permitted to do so under its contracts with those suppliers.

Despite any clause to the contrary, the Contractor represents and warrants that its services hereunder shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Agreement. For any breach of this warranty, the Contractor shall, for a period of ninety (90) days from performance of the service, perform the services again, at no cost to Customer, or if Contractor is unable to perform the services as warranted, Contractor shall reimburse Customer the fees paid to Contractor for the unsatisfactory services. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

IV. PAYMENT

A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)

Neb. Rev. Stat. §§81-2403 states, "[n]o goods or services shall be deemed to be received by an agency until all such goods or services are completely delivered and finally accepted by the agency."

B. TAXES (Statutory)

The State is not required to pay taxes and assumes no such liability as a result of this RFP. The Contractor may request a copy of the Nebraska Department of Revenue, Nebraska Resale or Exempt Sale Certificate for Sales Tax Exemption, Form 13 for their records. Any property tax payable on the Contractor's equipment which may be installed in a state-owned facility is the responsibility of the Contractor

C. INVOICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:

Please see Section 12 ("Payment") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

Also, as to Taxes, please see Exhibit A of the Nebraska Participating Addendum Contract 550001 04.

Invoices for payments must be submitted by the Contractor to the agency requesting the services with sufficient detail to support payment. Submit monthly invoices to: ocio.procurement@nebraska.gov. The terms and conditions included in the Contractor's invoice shall be deemed to be solely for the convenience of the parties. No terms or conditions of any such invoice shall be binding upon the State, and no action by the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

State, including without limitation the payment of any such invoice in whole or in part, shall be construed as binding or estopping the State with respect to any such term or condition, unless the invoice term or condition has been previously agreed to by the State as an amendment to the contract.

D. INSPECTION AND APPROVAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 19 ("Inspection") of the NASPO/WSCA Master Agreement.

Final inspection and approval of all work required under the contract shall be performed by the designated State officials.

The State and/or its authorized representatives shall have the right to enter any premises where the Contractor or subcontractor duties under the contract are being performed, and to inspect, monitor or otherwise evaluate the work being performed. All inspections and evaluations shall be at reasonable times and in a manner that will not unreasonably delay work.

E. PAYMENT (Statutory)

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 12 ("Payment") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2403). The State may require the Contractor to accept payment by electronic means such as ACH deposit. In no event shall the State be responsible or liable to pay for any goods and services provided by the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Contractor prior to the Effective Date of the contract, and the Contractor hereby waives any claim or cause of action for any such services.

F. LATE PAYMENT (Statutory)

The Contractor may charge the responsible agency interest for late payment in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2401 through 81-2408).

G. SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS (Statutory)

The State's obligation to pay amounts due on the Contract for a fiscal years following the current fiscal year is contingent upon legislative appropriation of funds. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal year(s) for which such funds are not appropriated. The State will give the Contractor written notice thirty (30) calendar days prior to the effective date of termination. All obligations of the State to make payments after the termination date will cease. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

AT&T Response:

Please see Exhibit A of the Nebraska Participating Addendum Contract 550001 04.

H. RIGHT TO AUDIT (First Paragraph is Statutory)

The State shall have the right to audit the Contractor's performance of this contract upon a thirty (30) days' written notice. Contractor shall utilize generally accepted accounting principles, and shall maintain the accounting records, and other records and information relevant to the contract (Information) to enable the State to audit the contract. (Neb. Rev. Stat. §84-304 et seq.) The State may audit and the Contractor shall maintain, the Information during the term of the contract and for a period of five (5) years after the completion of this contract or until all issues or litigation are resolved, whichever is later. The Contractor shall make the Information available to the State at Contractor's place of business or a location acceptable to both Parties during normal business hours. If this is not practical or the Contractor so elects, the Contractor may

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

provide electronic or paper copies of the Information. The State reserves the right to examine, make copies of, and take notes on any Information relevant to this contract, regardless of the form or the Information, how it is stored, or who possesses the Information. Under no circumstance will the Contractor be required to create or maintain documents not kept in the ordinary course of contractor's business operations, nor will contractor be required to disclose any information, including but not limited to product cost data, which is confidential or proprietary to contractor.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
			Please see Section 20 ("Inspection and Audit") of the NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04.

The Parties shall pay their own costs of the audit unless the audit finds a previously undisclosed overpayment by the State. If a previously undisclosed overpayment exceeds one percent (1%) of the total contract billings, or if fraud, material misrepresentations, or non-performance is discovered on the part of the Contractor, the Contractor shall reimburse the State for the total costs of the audit. Overpayments and audit costs owed to the State shall be paid within ninety (90) days of written notice of the claim. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

V. PROJECT DESCRIPTION AND SCOPE OF WORK

The bidder must provide the following information in response to this Request for Proposal.

A. PROJECT OVERVIEW

The objective of this section of the RFP is to identify a Contractor that will provide an Emergency / Mass Notification Service (hereafter known as EMNS) that will be used by all State agencies, boards and commissions (hereafter known as the State), and political subdivisions of the State, each with administrative rights to their respective division. This is a diverse group of clients that includes State and local agencies, departments, and institutions.

AT&T Response:

AT&T has read and understands.

B. PROJECT ENVIRONMENT

The State acquires this product, and associated services, then the Office of the Chief Information Officer (OCIO) makes them available to requesting subscribers on a cost recovery basis.

State Agencies that wish to use an EMNS will be obligated to use this shared service. The OCIO will also market this service to political subdivisions within the State. The potential exists for a large amount of growth of administrators, recipients and usage of this service.

Primarily, the EMNS shall have the 3 key following capabilities. The EMNS shall have the capability to send alerts or notifications to an identified set of users whose contact information is contained within an established and managed database. The EMNS shall have the capability to notify the general public within a defined geographic area. The general public shall not be required to enroll in an EMNS database in order to receive these notifications. The EMNS shall have the capability where users may voluntarily enroll and un-enroll from a database in order to receive or discontinue notifications and messages.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

The EMNS shall have the capability to fully support the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS). IPAWS automates and streamlines the process of issuing public alerts. IPAWS enables the federal, state, local tribal and territorial authorities the capability to issue critical public alerts and warnings. The EMNS must be compliant with all requirements outlined by IPAWS 2.0 and WEA 2.0. The Technical Requirements Matrix provides the specific requirements.

The EMNS provides designated administrators the ability to send time-sensitive alerts or messages to many devices via many methods. Possible supported devices of this service are listed below.

AT&T Response:

AT&T has read and understands.

1. DEVICES SUPPORTED

Software as a Service (SaaS) with the following devices supported:

a. Land line phones;

b. Voice over IP(VoIP);

c. Mobile phones/devices;

d. SMS text, text to mobile devices;

e. Mobile device apps;

f. Email;

g. Desktops;

h. Fax;

i. Social Media such as Facebook and Twitter, etc.;

j. TTY for hearing impaired.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

2. FEATURES

Features of the current service:

a. Toll free activation of notifications;

b. Answering machine detection;

c. On the fly message recording;

d. 24x7x365 tech support;

e. Multilanguage support (English, Spanish, French);

f. Notification attachments;

g. Polling abilities;

h. Conference call bridging capabilities;

i. International dialing;

j. On demand reports; this is a web-based system that includes API, automated escalation, notification initiation from phone, mobile phone or email, and;

k. Inbound calling.

3. RECIPIENTS/USERS

Initial anticipated number of recipients/users: 30,000 to 50,000.

4. CLIENTS SERVED

Current clients being served (known as divisions), each with administrative and initiator rights within their respective divisions.

a. Chadron State College;

b. Department of Agriculture;

c. Nebraska Department of Corrections;

d. Nebraska Department of Transportation;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

e. Nebraska Health and Human Services;

f. Nebraska Office of the Chief Information Officer (OCIO);

g. Nebraska State Historical Society;

h. Nebraska State Patrol;

i. Douglas County EMA;

j. Grand Island – Hall County EMA;

k. Hall County EMA;

l. Kearney County Health Services;

m. Sarpy County EMA;

n. Northeast Nebraska Public Health Department;

o. South Heartland – Two Rivers Public Health Department;

p. State of Nebraska (has statewide administrative and initiator rights over all divisions);

q. Wayne State College;

r. University of Nebraska-Lincoln, and;

s. NEMA.

C. SCOPE OF WORK

The bidder shall provide a reliable, robust, interactive, efficient and high speed EMNS. This service will be purchased as Software as a Service (SaaS) for the benefit of the State and any or all political subdivisions that may subscribe to this as a shared service through a statewide enterprise contract.

This service will be used by the State and any or all political subdivisions, each with administrative rights to their respective division. This is a diverse group of clients that includes State and local agencies/counties, departments, and educational institutions, etc.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

The EMNS service will allow for each political subdivision to select either service with or without telephony capabilities as defined in the General Service Requirements Item 1.1. Pricing for the service will be per enrolled contact depending on which of the two types of base service their respective agency chooses. The pricing level will depend on the total census count at the end of each month for the State of Nebraska to set the rate for that month. Billing from the contractor will be on a monthly total per contact of each of the two types of service to the State of Nebraska and the State of Nebraska will rebill monthly to each political subdivision on a cost recovery basis. Any additional services such as GIS mapping, optional products and services, or custom programming to meet end user needs will be billed to the State of Nebraska in whole and then rebilled to the political subdivision.

D. TECHNICAL REQUIREMENTS

See Attachment One for the Technical Requirements Matrix. The bidder's response must provide enough detail in narrative form to allow the Evaluation Committee to score the bidder's approach to each technical specification.

E. DELIVERABLES

The bidder must make available an Emergency Mass Notification Software as a Service which meets the technical specifications outlined previously in this document.

VI. PROPOSAL INSTRUCTIONS

This section documents the requirements that should be met by bidders in preparing the Technical and Cost Proposal. Bidders should identify the subdivisions of "Project Description and Scope of Work" clearly in their proposals; failure to do so may result in disqualification. Failure to respond to a specific requirement may be the basis for elimination from consideration during the State's comparative evaluation.

Proposals are due by the date and time shown in the Schedule of Events. Content requirements for the Technical and Cost Proposal are presented separately in the following subdivisions; format and order:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

A. PROPOSAL SUBMISSION

1. CORPORATE OVERVIEW

The Corporate Overview section of the Technical Proposal should consist of the following subdivisions:

a. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

AT&T Response:

Corporate Name

AT&T Mobility LLC.

Company's Headquarters

AT&T Corp. headquarters is One AT&T Way, Bedminster, NJ 07921.

Entity Organization

AT&T is an independent, publicly traded corporation, and no individual owns more than 10% of the company.

Headquartered in Dallas, Texas, we're investing to be a global leader in telecommunications, media, and technology. We offer innovative solutions for our customers and strong returns for our shareholders.

Incorporated

The AT&T Corp. date of incorporation was March 3, 1885.

The AT&T Corp. state of incorporation is New York.

The AT&T Mobility National Accounts, LLC incorporation date was December 2, 1999.

The AT&T Mobility National Accounts, LLC state of incorporation was Delaware.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Name Change

Since 2005, AT&T's ownership structure has been unchanged.

SBC acquired AT&T in 2005 and retained the AT&T name and brand. Since then, we've had no change in ownership.

b. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that proposal evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

The State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

AT&T Response:

AT&T Corp. is wholly owned subsidiary of AT&T, Inc. and a member of the AT&T Inc. family of companies. AT&T financial information is consolidated and reported at the AT&T Inc. level.

The most recent Annual Report for AT&T can be found in the Investor Relations section of our website at: http://www.att.com/gen/investor-relations?pid=9186

c. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the proposal due date, the bidder should describe the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded contractor(s) will require notification to the State.

AT&T Response:

AT&T is a publicly owned company, and does not comment on any corporate transactions except as allowed by applicable securities laws.

d. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

AT&T Response:

AT&T

161 Inverness Drive West

Englewood, CO 80112

e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous five (5) years. If the organization, its predecessor, or any Party named in the bidder's proposal response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

AT&T Response:

AT&T is currently working with the State of Nebraska under NASPO/WSCA Master Agreement and Exhibit A of the Nebraska Participating Addendum Contract 55001 04. Current services include wireline and mobility services.

f. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's proposal response is or was an employee of the State within the past thirty-six (36) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

If any employee of any agency of the State of Nebraska is employed by the bidder or is a subcontractor to the bidder, as of the due date for proposal submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this proposal. If no such relationship exists, so declare.

AT&T Response:

No such relationship exists or has existed.

g. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past five (5) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the contractor's non- performance or poor performance, and the issue was either not litigated due to inaction on the part of the contractor or litigated and such litigation determined the contractor to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past five (5) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's proposal accordingly. If no such termination for default has been experienced by the bidder in the past five (5) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

AT&T Response:

This question is overbroad and impossible to respond to accurately in any practical fashion.

AT&T Corp. is a large communications company with over 100 years in operation and a national [and international] presence. As such, it has contractual relationships throughout the world with numerous customers. Although AT&T is committed to

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

honoring its obligations to all of its customers, and makes every effort to comply, parties may differ. As such, it is likely that a customer has terminated a contract for cause or accepted damages in lieu of for cause termination; however, given the sheer size of the corporation and the number of jurisdictions where AT&T operates, it would be impossible to provide any more specific information at this time. Except for material matters that AT&T discloses in filings with the Securities and Exchange Commission or otherwise discloses in response to subpoenas or other valid court orders, AT&T is legally and contractually prohibited from disclosing information to third parties about contractual matters. Also, due to the size and scale of AT&T's operations, as a practical matter, AT&T cannot state with absolute certainty whether AT&T has defaulted under a contract. Notwithstanding the legal and practical restrictions that limit AT&T's ability to disclose specific contract performance issues, AT&T can assure the State that AT&T is capable of performing the services requested under this RFP and that AT&T has no history or pattern of performance issues with other customers that would affect AT&T's ability to perform the services requested by the State. AT&T reiterates that AT&T is not aware of any circumstances involving performance under another contract which would materially and adversely impact AT&T's ability to perform services for the State. Moreover, to the best of its knowledge, AT&T is not aware of any circumstance when AT&T was not awarded a bid due to non-performance concerns about AT&T by the entity sponsoring a particular procurement.

h. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the bidder's previous projects similar to this RFP in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the proposal.

The bidder should address the following:

i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this RFP. These descriptions should include:

   a) The time period of the project;

   b) The scheduled and actual completion dates;

   c) The Contractor's responsibilities;

   d) For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

e) Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a contractor performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

ii. Contractor and subcontractor(s) experience should be listed separately. Narrative descriptions submitted for subcontractors should be specifically identified as subcontractor projects.

iii. If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the Contractors above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

AT&T Response:

AT&T has been in business for more than 143 years. We serve millions of customers around the world, including global, national, mid-size, regional, and government customers. Currently we provide service for all of the Fortune 1000 companies.

We are proud to provide our customers with a strong product and service line, thanks to our focus on delivering the industry's most reliable service, most globally consistent portfolio, and the most advanced network management and security tools.

During negotiations or presentations, your AT&T account team will secure customer references.

Most customers do not wish to be contacted directly as references. So, your account team will work to arrange contact or to supply you with direct contact information.

Consequently, we're unable to provide you with customer references until that time.

i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this RFP. The names and titles of the team proposed for assignment to the State project should be identified in full, with a description of the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

team leadership, interface and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The State will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the RFPRFP in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the State.

AT&T Response:

AT&T shall employ and make available at reasonable times an adequate number of appropriately qualified and trained personnel, familiar with the State's operations and use of telecommunications services, to provide and support the State's use of the Services in accordance with the terms of AT&T's Response to this RFP. The identities and titles of specific persons, technical expertise, and their availability to provide and support the State's needs will be separately established by authorized representatives of AT&T, within the parameters of confidentiality limits, upon award of the RFP to AT&T.

j. SUBCONTRACTORS

If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

i. name, address, and telephone number of the subcontractor(s);

ii. specific tasks for each subcontractor(s);

iii. percentage of performance hours intended for each subcontract; and

iv. total percentage of subcontractor(s) performance hours.

AT&T Response:

At this stage, AT&T is not able to specifically identify the subcontractors required for your solution. We reserve the right to engage subcontractors as needed for installation

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

and maintenance services; however, all contracting with you will be directly with AT&T. We will identify any third-party providers during the negotiation phase.

We select our subcontractors with the goal to provide the best service to you. Upon award AT&T will work with your Procurement and AT&T Strategic Sourcing to validate any third parties.

2. TECHNICAL APPROACH

The technical approach section of the Technical Proposal should consist of the following subsections:

a. Understanding of the project requirements;

b. Proposed development approach;

c. Technical considerations;

d. Detailed project work plan; and

e. Deliverables and due dates.

AT&T Response:

AT&T has read and understands.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Form A
Contractor Proposal Point of Contact

Request for Proposal Number 6214 Z1

Form A should be completed and submitted with each response to this RFP. This is intended to provide the State with information on the contractor's name and address, and the specific person(s) who are responsible for preparation of the bidder's response.

Preparation of Response Contact Information	
Bidder Name:	AT&T Mobility LLC.
Bidder Address:	161 Inverness Dr W, Englewood CO 80112
Contact Person & Title:	Micah Cogan, Client Solutions Executive
E-mail Address:	micah.m.cogan@att.com
Telephone Number (Office):	720-628-4605
Telephone Number (Cellular):	
Fax Number:	

Each bidder should also designate a specific contact person who will be responsible for responding to the State if any clarifications of the bidder's response should become necessary. This will also be the person who the State contacts to set up a presentation/demonstration, if required.

Communication with the State Contact Information	
Bidder Name:	AT&T Mobility LLC.
Bidder Address:	161 Inverness Dr W, Englewood CO 80112
Contact Person & Title:	Micah Cogan, Client Solutions Executive
E-mail Address:	micah.m.cogan@att.com
Telephone Number (Office):	720-628-4605
Telephone Number (Cellular):	
Fax Number:	

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Request for Proposal for Contractual Services form, the bidder guarantees *** subject to and to the extent specified in AT&T's Proposal Response *** compliance with the procedures stated in this RFP, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

CW NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this RFP.

CW I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

CW I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD (NOT ELECTRONICALLY)

FIRM:	AT&T Mobility LLC.
COMPLETE ADDRESS:	161 Inverness Dr W, Englewood CO 80112
TELEPHONE NUMBER:	618-604-9063
FAX NUMBER:	
DATE:	February 07, 2020
SIGNATURE:	

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Request for Proposal for Contractual Services form, the bidder guarantees ***** subject to and to the extent specified in AT&T's Proposal Response ***** compliance with the procedures stated in this RFP, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

_____ NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this RFP.

_____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD (NOT ELECTRONICALLY)

FIRM:	**AT&T Mobility LLC.**
COMPLETE ADDRESS:	**161 Inverness Dr W, Englewood CO 80112**
TELEPHONE NUMBER:	**618-604-9063**
FAX NUMBER:	
DATE:	**February 07, 2020**
SIGNATURE:	

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

TYPED NAME & TITLE OF SIGNER: Chris Wilson, Regional Sales Manager

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Attachments:

- State of Nebraska WSCA
- Master Service Agreement
- Business Continuity Handbook

Additional Attachments:

- Technical Requirement Matrix
- Cost Proposal
- Rave Platform Architecture and Operational Security Overview

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

STATE OF NEBRASKA SERVICE CONTRACT AWARD

State Purchasing Bureau
301 Centennial Mall South, 1st Floor
Lincoln, Nebraska 68508
OR
P.O. Box 94847
Lincoln, Nebraska 68509-4847
Telephone: (402) 471-2401
Fax: (402) 471-2089

PAGE	ORDER DATE
1 of 1	01/31/13
BUSINESS UNIT	BUYER
65060014	MARY LANNING (AS)

VENDOR NUMBER: 2045026

VENDOR ADDRESS:

AT&T MOBILITY NATIONAL ACCOUNTS LLC
DBA AT & T MOBILITY
7229 PARKWAY DR
HANOVER MARYLAND 21076-1317

CONTRACT NUMBER
55001 O4

AN AWARD HAS BEEN MADE TO THE VENDOR/CONTRACTOR NAMED ABOVE FOR THE SERVICES AS LISTED BELOW FOR THE PERIOD:

FEBRUARY 01, 2013 THROUGH OCTOBER 31, 2016

THIS CONTRACT IS NOT AN EXCLUSIVE CONTRACT TO FURNISH THE SERVICES SHOWN BELOW, AND DOES NOT PRECLUDE THE PURCHASE OF SIMILAR SERVICES FROM OTHER SOURCES.

THE STATE RESERVES THE RIGHT TO EXTEND THE PERIOD OF THIS CONTRACT BEYOND THE TERMINATION DATE WHEN MUTUALLY AGREEABLE TO THE VENDOR/CONTRACTOR AND THE STATE OF NEBRASKA.

Originally awarded from WSCA Contract 1907

Contract to supply and deliver AT&T Wireless Voice Service, Wireless Broadband Service, Accessories and Equipment, through a prime vendor program to State of Nebraska agencies for the period February 1, 2013 through October 31, 2016 with the option to renew for one (1) additional two (2) year periods, per the terms, conditions and specification of the " Request for Proposal".

Payment: 45 days

Purchase Orders for State Agencies, Boards and Commissions for AT&T National Mobility Accounts LLC must be processed by Administrative Services, Office of the OCIO. Political Subdivisions are responsible for processing Purchase Order directly with the contracted vendor.

(For the File - This RFP and Contract are bid and awarded by the State of Nevada. All backup bids, etc. are retained by the Nevada Department of Administration, State Procurement Office).

(For the File: The WSCA/AT&T National Mobility Accounts LLC Master Price Agreement contract period was effective April 10, 2012. The WSCA Participating Addendum for Nebraska became effective on February 1, 2013).

Vendor Contact: Michael Lewis
Phone: 785-691-6469
Email: mike.lewis@att.com

(01/31/13 djg)

Line	Description	Quantity	Unit of Measure	Unit Price	Extended Price
1	WIRELESS VOICE AND DATA SERVICES	150,000.0000	EA	1.0000	150,000.00
	Total Order				**150,000.00**

BUYER 2/1/13

MATERIEL ADMINISTRATOR 2-7-13

bp/ks 2-4-13

PARTICIPATING ADDENDUM
UNDER THE
WESTERN STATES CONTRACTING ALLIANCE
WIRELESS COMMUNICATION SERVICES AND EQUIPMENT
BID NUMBER RFP: #S1907

PARTICIPANT: State of Nebraska

This Participating Addendum (the "PA") is made this First day of February, 2013 (the "PA Effective Date"), between the State of Nebraska ("Participant"), and AT&T Mobility National Accounts LLC ("Contractor") (Participant and Contractor are, at times, referred to individually as a "Party" or together as the "Parties").

Section 1. Recitals.

1.1 Contractor and the State of Nevada, acting through its Department of Administration, Purchasing Division, and the participating members of the Western States Contracting Alliance ("WSCA"), and the NASPO Cooperative, are parties to that certain Western States Contracting Alliance contract, #S1907, dated March 15, 2012, successor contract to that certain Western States Contracting Alliance contract number 1523, dated October 10, 2006, as amended, successor contract to that certain Western States Contracting Alliance contract number 10-00115, dated June 29, 2001, as amended (the "Contract").

1.2 Participant wants to participate in the Contract pursuant to the terms and conditions of this PA.

Section 2. Agreement. In consideration of the recitals set forth in §1 above, which are hereby re-stated and agreed to by the Parties, and for valuable consideration, the receipt and sufficiency of which is hereby acknowledged by the Parties, Participant and Contractor hereby agree to the terms and conditions of this PA (the Contract and the PA, together with all Purchase Orders submitted to Contractor by Participating Entity, collectively, the "Agreement"). Unless otherwise defined, capitalized terms in this PA have the meanings ascribed to them in the Contract.

Section 3. Authorized Participating Entities. Participant hereby designates: All State, county, cities, public schools, colleges or universities and all tax supported entities as the only authorized Participating Entity(ies) under the Agreement.

Section 4. Purchase Orders. Participating Entity(ies) must issue purchase orders hereunder that reference both Master Agreement #S1907 and the PA. Upon issuance of any such valid purchase order, Participating Entity will be bound by the terms and conditions of the Agreement including, without limitation, the obligation to pay Contractor for Service and Equipment provided. Notwithstanding the foregoing, purchase orders submitted that do not properly reference the Master Agreement number and/or the Participating Addendum may be accepted, at AT&T's sole discretion, if AT&T can reasonably ascertain that such purchase order was properly authorized and intended for use with the Participating Addendum. In such instances, the corresponding purchase order will be similarly valid and binding.

Section 5. Primary Contacts.

Participant:

Name: Mary Lanning
Title: Buyer
Address: 301 Centennial Mall South
Lincoln NE 68508
Telephone: 402-471-0973
Fax Number: 402-471-2089
E-Mail: mary.lanning@nebraska.gov

Lead State:

Name: Teri Smith
Title: Purchasing Officer
Address: 515 E. Musser St., Suite 300
Carson City, NV 89701
Telephone: 775-684-0178
Fax Number: 775-684-0188
E-Mail: tlsmith@admin.nv.gov

Contractor Account Team:

Name: Michael Lewis
Title: Account Manager
Address:

Telephone: 785 691 6469
Fax Number:
E-Mail: mike.lewis@att.com

Contractor Main:

Name: Twila Lively
Title: Manager, Sales Operations
Address: 2600 Camino Road
San Ramon, CA 94583
Telephone: (925) 487-9945
Fax Number: (510) 261-2155
E-Mail: twilalively@att.com

Section 6. Authority. By signing below, the corresponding Party's representative represents that such person is duly authorized by Contractor or Participant, as applicable, to execute this PA on behalf of the respective Party, and that the Contractor and Participant agree to be bound by the provisions hereof. In addition, Participant represents that it has received the requisite approvals from the applicable Chief Procurement Official and WSCA to participate in the Agreement.

Section 7. Miscellaneous.

7.1 American Recovery and Reinvestment Act of 2009 ("ARRA"). If or when Contractor is notified in writing by ordering entity that a specific purchase or purchases are being made with ARRA funds, Contractor agrees to comply with the data element and reporting requirements as currently defined in Federal Register Vol 74 #61, Pages 14824-14829 (or subsequent changes or modifications to these requirements as published by the Federal OMB) that are legally required of vendors as providers of goods and services to recipients or sub-recipients of ARRA funds. Each Participating Entity is responsible for informing Contractor in writing prior to ARRA funds being used for a purchase or purchases under the Contract. Contractor will provide the required report, if any, to the ordering entity with the invoice presented to the Participating Entity for payment. Contractor will provide the required report, if any, to the Participating Entity with the invoice presented to the Participating Entity for payment. Contractor, as it relates to purchases under the Contract, is not a sub-contractor, recipient, sub-recipient or sub-grantee, but simply a vendor, as defined in the OMB guidelines, and assumes no responsibilities under ARRA beyond those required of a vendor.

Section 8. **Notice of Administration Fees.** Participant and any and all other Participating Entities under this PA are hereby on notice of the following administration fees being paid by Contractor under the Contract.

- **WSCA.** Contractor has included in the price offered a WSCA Administration Fee of 1/10th of 1% (one-tenth of one percent) of the Total Wireless Spend, pursuant to the schedule of payments set forth in the Contract.
- **State of Nebraska Contractor has included in the price offered** an Administration Fee of 1/10th of 1% (one-tenth of one percent) of the Total Wireless Spend pursuant to the schedule of payments set forth in the schedule described here in the Participating Addendum. The Contractor shall submit quarterly reports to the Participant's Contract Administrator or designee 45 days after the end of the quarter as described here in the calculation of the Administration Fee.

Quarter`	Period	Due Date
1	January - March	May 15
2	April – June	August 15
3	July – September	November 15
4	October – December	February 15

"Total Wireless Spend" means, with respect to the Administration Fee, the total amount of the charges set forth on the invoices sent by Contractor to Participating Entities under the Participating Addendum, less taxes and surcharges.

Section 9. **Order of Precedence.** The Parties acknowledge and agree that in the event of a conflict between the terms contained in the various documents comprising this Agreement, the following order of precedence will control: (a) this PA; (b) the Master Agreement; and (c) any Purchase Order issued in connection therewith. This section specifically supersedes any order of precedence provisions set forth elsewhere in the Agreement.

Section 10. **Additional Terms and Conditions.** The Parties acknowledge and agree to the additional terms and conditions set forth in Exhibit A, attached hereto and incorporated herein by reference.

Section 11. **Entire Agreement.** The Agreement sets forth the entire agreement between the Parties with respect to the subject matter of all previous communications, representations or agreements, whether oral or written, with respect to the subject matter hereof. Except as expressly provided in the Agreement, terms and conditions inconsistent with, contrary or in addition to the terms and conditions of the Agreement shall not be added to or incorporated herein by any subsequent purchase order; and any such attempts to add or incorporate such terms and conditions are hereby rejected. The terms and conditions of the Agreement shall prevail and govern in the case of any such inconsistent or additional terms.

IN WITNESS WHEREOF, the Parties have executed this PA as of the PA Effective Date.

STATE OF NEBRASKA

By: _____, duly authorized

Name: Bo Botelho

Title: AS Materiel Administrator

Date: 2-4-13

AT&T MOBILITY NATIONAL ACCOUNTS LLC

By: _____, duly authorized

Name: Linda J Cottingham

Title: Sr. Contract Manager

Date: 1/11/13

EXHIBIT A

ADDITIONAL TERMS AND CONDITIONS

Changes

TAXES of the Standard Terms and Conditions shall read as follows:
The State of Nebraska is exempt from the obligation to pay federal excise taxes; it is further exempt by state law, Neb. Rev. Stat. § 2704.15, from the obligation to pay sales and use taxes. Taxes must not be included in the bid prices. Exemption by statute precludes the obligation to furnish a State of Nebraska exemption certificate. Copies of exemption certificates may be attached hereto as a courtesy.

REPORTS of the Standard Terms and Conditions shall contain additional language as follows:
The Contractor shall also provide to the State of Nebraska primary contact person quarterly utilization reports containing at a minimum the following information pertaining to State of Nebraska utilization: (a) purchase order number; (b) description; (c) quantity; and (d) price. These reports will be provided in Excel format and sent via email on a quarterly basis as follows:

Period End	Report Due
December 31	January 31
March 31	April 30
June 30	July 31
September 30	October 31

DELIVERY OF GOODS shall be added as follows:
No payment shall be made for any Products or Services until the Purchasing Entity has accepted the Products or Services. The Purchasing Entity will make every effort to notify the Contractor of non-acceptance within fifteen (15) days of delivery of a Product or Service; failing which the Product or Service shall be deemed accepted by the Purchasing Entity

PROMPT PAYMENT of the Standard Terms and Conditions shall read as follows:
The State of Nebraska will make payments in strict accordance with the Nebraska Prompt Payment Act, Neb. Rev. Stat. § 81-2401 et seq., as described in Neb. Rev. Stat. § 81-2403 of the Act. Interest charges may be assessed for late payments in accordance with § 81-2404 of the Act. Payments are due upon receipt of an undisputed invoice, merchandise or service, whichever is later, and payable in accordance with the Act unless otherwise specified in a Transaction Document.

The State of Nebraska may terminate this Contract or any purchase order, in whole or in part, in the event funding is no longer available. Its obligation to pay amounts due for fiscal years following the current fiscal year is contingent upon legislative appropriation of funds for this contract. Should said funds not be appropriated, the State of Nebraska may terminate this Contract or any purchase order with respect to those payments for the fiscal years for which such funds are not appropriated. The State of Nebraska will give the Contractor written notice of thirty (30) days prior to the effective date of any termination under this section. All obligations of the State of Nebraska to make payments after the termination date will cease and all interest of the State of Nebraska in any related equipment will terminate. The Contractor shall be entitled to receive just and fair compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

RECORDS ADMINISTRATION AND AUDIT OF RECORDS of the Standard Terms and Conditions shall be amended to read as follows:
These records shall be maintained for a period of five (5) full years from the date of final payment, or until all issues related to an audit, litigation or other action are resolved, whichever is longer. All records shall be maintained in accordance with generally accepted accounting principles.

DRUG POLICY shall be added as follows:
Drug Policy: Contractor certifies, by signing this agreement that it maintains a drug free work place environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon written request by the State of Nebraska.

NEW EMPLOYEE WORK ELIGIBILITY STATUS shall be added as follows:
The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of new employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of a newly hired employee.

If the Contractor is an individual or sole proprietorship, the following applies:

A. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at www.das.state.ne.us.

B. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

CONTRACT MONITORING shall be added as follows:
The contractor is obligated to furnish information as requested to determine whether the objectives of the contract have been met. The contractor will be required to furnish quarterly reports to the State of Nebraska primary contact upon request.

FUNDING OUT CLAUSE OR LOSS OF APPROPRIATIONS
The State may terminate the contract, in whole or in part, in the event funding is no longer available. The State's obligation to pay amounts due for fiscal years following the current fiscal year is contingent upon legislative appropriation of funds for the contract. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal years for which such funds are not appropriated. The State will give the contractor written notice thirty (30) days prior to the effective date of any termination, and advise the contractor of the location (address and room number) of any related equipment. All obligations of the State to make payments after the termination date will cease and all interest of the State in any related equipment will terminate. The contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the contractor be paid for a loss of anticipated profit.

For Purchasing Use Only:

RFP/CONTRACT # 1907

MASTER SERVICE AGREEMENT

A Contract between the Western States Contracting Alliance
Acting by and through the State of Nevada

and

AT&T MOBILITY NATIONAL ACCOUNTS LLC

RECITALS

Whereas, pursuant to Nevada Revised Statute (NRS) 277.100, NRS 277.110, NRS 333.162(1)(d), and NRS 333.480 the Chief of the Purchasing Division of Nevada is authorized to enter into cooperative group-contracting consortium;

Whereas, WSCA issued Request for Proposal #1907 for Wireless Voice Service, Wireless Broadband Service, Accessories and Equipment, dated February 3, 2011, as amended, which is attached hereto and incorporated herein as Attachment BB (the "Solicitation");

Whereas, Contractor submitted its Response to the Solicitation, which is attached hereto and incorporated herein as Attachment CC (the "Response");

Whereas, on or about May 24, 2011, and in connection with the Solicitation, WSCA gave notice of its intent to award contracts to certain entities including Contractor (the "Notice of Intent to Award");

Whereas, WSCA and Contractor intend to enter into a contract in connection with the Solicitation and the Notice of Intent to Award that operates to both (a) set forth terms and conditions applicable between WSCA and/or the Lead State, and Contractor with respect to the overall procurement; and (b) set forth the primary, first-in-precedence terms and conditions applicable between Contractor and Participating Entities participating in the Contract.

In consideration of the above premises, and for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties mutually agree as follows:

1. REQUIRED APPROVAL. The Master Service Agreement (aka the "Contract") shall not become effective until and unless approved by the WSCA Directors.

2. DEFINITIONS.

2.1 "Contract" and "Master Service Agreement" mean this document, entitled "Master Service Agreement," including, without limitation, Contractor's Special Terms and Conditions, as may be amended by the Lead State, and Contractor, together with other incorporated documents as more fully described in §5 herein.

2.2 "Contractor" means the vendor entity that, along with WSCA, is a party to the Contract and that performs services and/or provides goods for WSCA under the Contract.

2.3 "Fiscal Year" is the Lead State's fiscal year, which is the period beginning July 1 and ending June 30 of the following year.

2.4 "Participant" and/or "Participating State" means a state or other authorized entity that (a) has executed a Participating Addendum; or (b) has signed (and not revoked) an Intent to Contract at the time of the award of this Contract.

2.5 "Participating Addendum" and/or "PA" mean an agreement between Contractor and a Participant, in form and substance substantially similar to Exhibit 1 to the Special Terms and Conditions, through which such Participant participates in the Contract.

2.6 "Participating Entity" and/or "Buyer" mean a Participant, Participating State or other entity properly authorized by a Participant to purchase services and products under the Contract, or that otherwise participates in the Contract through the corresponding Participating Addendum.

2.7 "Special Terms and Conditions" means Contractor's additional terms and conditions, unique to Contractor with respect to its corresponding services and products, which are attached hereto and incorporated herein as Attachment AA.

2.8 "State" and/or "Lead State" means the State of Nevada and its state agencies, officers, employees and immune contractors as defined in NRS 41.0307, and for purposes of this Contract, the Lead State is acting on behalf of WSCA with the authority to enter into, and amend the Contract.

2.9 "Sub-PA" means a document executed by a Participating Entity participating in an existing PA pursuant to which separate terms and conditions applicable only to that Participating Entity and other authorized entities.

2.10 "Total Wireless Spend" means, with respect to the WSCA Administration Fee, the total amount of the charges set forth on the invoices sent by Contractor to Participating Entities under the Contract, less taxes and surcharges.

2.11 "WSCA" means the Western States Contracting Alliance, a cooperative group-contracting consortium for state government departments, institutions, agencies and political subdivisions (i.e.,

colleges, school districts, counties, cities, etc.,) for the states of Alaska, Arizona, California, Colorado, Hawai'i, Idaho, Minnesota, Montana, Nevada, New Mexico, Oregon, South Dakota, Utah, Washington and Wyoming.

3. **CONTRACT TERM.** The Contract shall be effective from March 15, 2012 to October 31, 2016, (subject to the WSCA Directors' approval), unless sooner terminated by either Party as specified in paragraph 21 herein. Each Participating Addendum executed in connection with the Contract shall be effective from its corresponding effective date through the end of the Contract's term, unless otherwise specified in that Participating Addendum. Notwithstanding the foregoing, Contractor and the Lead State acknowledge and agree that Contractor may enter into a Participating Addendum with any Participant hereunder on or after this Contract's "effective from "date upon approval of the Lead State. Any such Participating Addendum so executed will be subject to the terms and conditions of this Contract.

4. **CANCELLATION; NOTICE.** The Contract may be canceled by either the Lead State or Contractor upon written notice sixty (60) days prior to the effective date of the cancellation. Cancellation of the Contract due to Contractor's default may be immediate. Further, any Participant may cancel its Participating Addendum upon thirty (30) days written notice to Contractor, unless otherwise limited or stated in the Participating Addendum. Any cancellation under this provision (a) may be in whole or in part; and (b) shall not effect the rights and obligations attending orders outstanding at the time of cancellation, including any right of any Participating Entity to indemnification by the Contractor, rights of payment for goods/services delivered and accepted, and rights attending any warranty or default in performance in association with any order.

5. **INCORPORATED DOCUMENTS; ORDER OF PRECEDENCE.** The Contract consists of this document, entitled "Master Service Agreement," together with the following incorporated documents; Contractor's Special Terms and Conditions, the Solicitation, and the Response. The document entitled Master Service Agreement together with the Contractor's Special Terms and Conditions are intended by the Parties to be the primary Participating Entity-facing contractual document in connection with the Solicitation. To participate in the Contract, each Participating Entity must do so pursuant to a Participating Addendum. In the event of any conflict between the terms and conditions of any of the documents comprising or related to the Contract, the following order of precedence will control:

1. The applicable Participating Addendum and/or Sub-PA;
2. The Master Service Agreement;
3. Contractor's Special Terms and Conditions (Attachment AA);
4. The Solicitation (Attachment BB);
5. The Response (Attachment CC);
6. Any individual order placed on the Contract by a Participating Entity

Notwithstanding the foregoing, Contractor and WSCA expressly acknowledge and agree that the terms and conditions unique to the states of Arizona, Montana, Oregon, and Utah, which were included under Attachment K of the Solicitation, were for informational purposes only and are NOT incorporated into the Contract by inclusion in the Solicitation.

The parties acknowledge and agree that each Participating Addendum executed in accordance herewith incorporates the terms and conditions of the Contract, and that the corresponding Participating Entities will be bound to the terms and conditions of that Participating Addendum and the Contract.

Neither the Special Terms and Condition, nor any purchase order(s) issued under the Contract shall contradict or supersede any terms and conditions in the Contract without written evidence of mutual assent to such change(s) between Contractor and the Lead State.

6. [OMITTED]

7. **ASSENT.** The parties agree that the terms and conditions listed on incorporated attachments of this Contract are also specifically a part of this Contract and are limited only by their respective order of precedence and any limitations specified.

8. [OMITTED]

9. [OMITTED]

10. [OMITTED]

11. **CONSIDERATION.** The parties agree that Contractor will provide the services and products specified in, and in accordance with the Contract. Contracted prices represent ceiling prices for the supplies and services offered. Contractor shall report to the Lead State any price reduction or discount, or other more favorable terms offered to any Participating Entity and the Contractor agrees to negotiate in good faith to re-establish ceiling prices or other more favorable terms and conditions applicable to future orders. Bid prices must remain firm for the full term of the Contract. In the case of error in the extension of prices in the bid, the unit prices will govern. WSCA does not guarantee to purchase any amount under this Contract. Estimated quantities in the Solicitation are for bidding purposes only and are not to be construed as a guarantee to purchase any amount. If Contractor has quoted a cash discount based upon early payment; discounts offered for less than thirty (30) days have not been considered in making the award. WSCA is not liable for any costs incurred by the bidder in proposal preparation.

12. **PAYMENT.** Payment is normally made within thirty (30) days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After forty-five (45) days the Contractor may assess overdue account charges up to a maximum rate of one (1) percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a Participating State's "Purchasing Card."

13. **TAXES.**

13.1 Payable By Participating Entities. Prices shall be exclusive of state sales and federal excise taxes. Participating Entities may be required to show proof of any tax exemptions. Where a

Participating Entity is not exempt from sales taxes on sales within its state, such Participating Entity will be liable for such taxes, and Contractor shall add the sales taxes on the billing invoice as a separate entry.

13.2 Payable by Contractor. Contractor will be responsible to pay all taxes, assessments, fees, premiums, permits, and licenses required by law for it to pay. The Lead State's applicable real property and personal property taxes are the responsibility of Contractor in accordance with NRS 361.157 and NRS 361.159. Contractor agrees to be responsible for payment of any such applicable government obligations not paid by its subcontractors during performance of this Contract. The Lead State may set-off against consideration due any delinquent government obligation owed the Lead State in accordance with NRS 353C.190.

14. FINANCIAL OBLIGATIONS OF PARTICIPATING ENTITIES. Participating Entities' financial obligations are limited to such entities having available funds. Participants incur no financial obligations on behalf of political subdivisions. Unless otherwise specified in the Solicitation, the resulting award(s) will be permissive.

15. ORDER NUMBERS. To the extent described in the Response, Contract order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

16. WSCA ADMINISTRATION FEE; REPORTS. The Contractor will pay WSCA an Administration Fee of $1/10^{th}$ of 1% (one-tenth of one percent) of the Total Wireless Spend, pursuant to the schedule of payments set forth in the Solicitation and Attachment G thereto. The Contractor shall submit quarterly reports to the WSCA Contract Administrator in accordance with the requisites of Attachment G to the RFP.

17. DELIVERY. The prices bid shall be the delivered price to any Participating Entity. All deliveries shall be F.O.B. destination with all transportation and handling charges paid by the Contractor. Responsibility and liability for loss or damage shall remain with the Contractor until final inspection and acceptance, when responsibility shall pass to the Participating Entity except as to latent defects, fraud and Contractor's warranty obligations.

18. HAZARDOUS CHEMICAL INFORMATION. The Contractor will provide one set of the appropriate material safety data sheet(s) and container label(s) upon delivery of a hazardous material to any Participating Entity. All safety data sheets and labels will be in accordance with each Participating State's requirements.

19. INSPECTIONS. Goods furnished under the Contract shall be subject to inspection and test by the Participating Entity at times and places determined by the Participating Entity. If the Participating Entity finds goods furnished to be incomplete or in non-compliance with the Contract, the Participating Entity may reject the goods and require Contractor to either correct them without charge or deliver them at a reduced price which is equitable under the circumstances. If Contractor is unable or refuses to correct such goods within a time deemed reasonable by the Participating Entity, the Participating Entity may cancel

the order in whole or in part. Nothing in this paragraph shall adversely affect the Participating Entity's rights including the rights and remedies associated with revocation of acceptance under the Uniform Commercial Code.

20. INSPECTION & AUDIT.

20.1 WSCA's Rights. The inspection and audit provisions of this §20.1 run to the benefit of WSCA, not to Participating Entities.

a. Books and Records. Contractor will maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the Contractor for costs authorized by the Contract. Contractor agrees to keep and maintain under generally accepted accounting principles (GAAP) full, true and complete records, contracts, books, and documents as are necessary to fully disclose to WSCA, the Lead State or United States Government, or their authorized representatives, upon audits or reviews, sufficient information to determine compliance with all state and federal regulations and statutes.

b. Inspection & Audit. Contractor agrees that the relevant books, records (written, electronic, computer related or otherwise), including, without limitation, relevant accounting procedures and practices of Contractor or its subcontractors, financial statements and supporting documentation, and documentation related to the work product shall be subject, at any reasonable time, to inspection, examination, review, audit, and copying at any office or location of Contractor where such records may be found, with or without notice by WSCA; the United States Government; the State Auditor or its contracted examiners, the Department of Administration, Budget Division, the Nevada State Attorney General's Office or its Fraud Control Units, the State Legislative Auditor, and with regard to any federal funding, the relevant federal agency, the Comptroller General, the General Accounting Office, the Office of the Inspector General, or any of their authorized representatives. All subcontracts shall reflect requirements of this paragraph.

c. Period of Retention. All books, records, reports, and statements relevant to this Contract must be retained a minimum four (4) years after the Contract terminates or or until all audits initiated within the four (4) years have been completed, whichever is later, and for five (5) years if any federal funds are used in the Contract. The retention period runs from the date of payment for the relevant goods or services by the State, or from the date of termination of the Contract, whichever is later. Retention time shall be extended when an audit is scheduled or in progress for a period reasonably necessary to complete an audit and/or to complete any administrative and judicial litigation which may ensue.

20.2 Participating Entities' Rights. Contractor will provide each Participating Entity with reasonable access to Contractor's books and records related to the corresponding Participating Entity's payments and participation in the Contract.

21. DEFAULT; REMEDIES.

21.1. WSCA's Rights Upon Default. Any of the following events shall constitute cause for WSCA to declare Contractor in default of the Contract: (1) nonperformance of contractual requirements under the Contract; and/or (2) a material breach of any term or condition of the Contract. In order to declare Contractor in default, WSCA shall issue a written notice of default providing a period in which Contractor shall have a reasonable opportunity to cure the default(s). Time allowed for cure shall not diminish or eliminate Contractor's liability for damages otherwise available under the Contract. If the default remains after Contractor has been provided the opportunity to cure, WSCA may do one or more of the following: (1) exercise any remedy provided by law; (2) terminate the Contract or portions thereof; and/or (3) suspend Contractor from receiving future bid solicitations.

21.2 Participating Entity's Rights Upon Default. Any of the following events shall constitute cause for a Participating Entity to declare Contractor in default of the corresponding Participating Addendum or Sub-PA: (1) non-performance of contractual requirements; and/or (2) Contractor's material breach of any term or condition of the Participating Addendum or Sub-PA. In order to declare Contractor in default, a Participating Entity shall issue a written notice of default providing a period in which Contractor shall have a reasonable opportunity to cure the default(s). Time allowed for cure shall not diminish or eliminate Contractor's liability for damages otherwise available under the Participating Addendum. If the default remains after Contractor has been provided the opportunity to cure, the Participating Entity may do one or more of the following: (1) exercise any remedy provided by law; (2) terminate the Participating Addendum, Sub-PA, or portions thereof.

21.3 No Cross Termination. Notwithstanding the foregoing, in the event of a default by Contractor hereunder, then (a) an individual Participating Entity may not terminate the Contract but, instead, may only terminate its own PA; (b) WSCA may not terminate an individual Participating Addendum or Sub-PA, except as a consequence of its termination of the Contract; and (c) a Participating Entity that is not (i) concurrently the Participant or Participating State under the corresponding Participating Addendum, or (ii) a party to a valid Sub-Participation Addendum, may not terminate the corresponding Participating Addendum or Sub-PA and, instead may only terminate any outstanding, unfilled purchase orders made in connection with the corresponding Participating Addendum or Sub-PA.

21.4 Post-Termination Issues. In the event of termination of the Contract or a Participating Addendum for any reason, the parties agree that the provisions of this paragraph survive termination:

a. The parties shall account for and properly present to each other all claims for fees and expenses and pay those which are undisputed and otherwise not subject to set off under the Contract. Neither party may withhold performance of winding up provisions solely based on nonpayment of fees or expenses accrued up to the time of termination;

b. Contractor shall satisfactorily complete work in progress at the agreed rate (or a pro rata basis if necessary) if so requested by WSCA or a Participating Entity;

c. Contractor shall execute any documents and take any actions necessary to effectuate an assignment of this contract if so requested by WSCA;

d. Contractor shall preserve, protect and promptly deliver into WSCA's possession all of WSCA's proprietary information in accordance with paragraph (31).

22. **REMEDIES NON-EXCLUSIVE.** Except as otherwise provided for by law or this Contract, the rights and remedies of the parties shall not be exclusive and are in addition to any other rights and remedies provided by law or equity, including, without limitation, actual damages, and to a prevailing party reasonable attorneys' fees and costs. It is specifically agreed that reasonable attorneys' fees shall include without limitation $125 per hour for attorneys employed by the Lead State. The Lead State may set off consideration against any unpaid obligation of Contractor to Lead State in accordance with NRS 353C.190, or the applicable Participating Addendum. A Participating Entity's right of set-off shall be in accordance with the law of the Participating Entity's state, and the provisions of the applicable Participating Addendum.

23. **LIMITED LIABILITY.** The Lead State will not waive and intends to assert available NRS chapter 41 liability limitations in all cases. Contract liability of Contractor, WSCA, the Lead State, and/or any and all Participating Entities shall not be subject to punitive damages. In no event shall Contractor be liable for inability of users to access 911 or E911 service. In no event shall either Contractor, WSCA, the Lead State and/or any and all Participating Entities be liable for any indirect, special, consequential or incidental damages, however caused, which are incurred by the other party and which arise out of any act or failure to act relating to this agreement, even if such party has been advised of the claim or potential claim or the possibility of such damages, and in no event shall either party be liable to the other party for punitive damages.

24. **FORCE MAJEURE.** Neither party to this Contract shall be deemed to be in violation of this Contract if it is prevented from performing any of its obligations hereunder due to strikes, failure of public transportation, civil or military authority, act of public enemy, accidents, fires, explosions, or acts of God, including, without limitation, earthquakes, floods, winds, or storms. In such an event the intervening cause must not be through the fault of the party asserting such an excuse, and the excused party is obligated to promptly perform in accordance with the terms of the Contract after the intervening cause ceases. WSCA may terminate this Contract after determining such delay or default will reasonably prevent successful performance of the Contract.

25. **INDEMNIFICATION.**

25.1 Contractor's Obligations to WSCA. To the fullest extent permitted by law, Contractor shall indemnify, hold harmless and defend, not excluding the Lead State's right to participate, the Lead State and/or WSCA from and against all liability, claims, actions, damages, losses, and expenses, including, without limitation, reasonable attorneys' fees and costs, arising out of any alleged negligent or willful acts or omissions of Contractor, its officers, employees and agents.

25.2 Contractor's Obligations to Participating Entities. The Contractor shall release, protect, indemnify and hold Participating Entities and their officers, agencies, employees, harmless from and against any damage, cost or liability, including reasonable attorney's fees for any or all injuries to persons, property or claims for money damages arising from acts or omissions of the contractor, his employees or subcontractors or volunteers.

25.3 Exception. Contractor will not be liable for damages that are the result of negligence or willful misconduct by WSCA, the Participating Entities, and/or their respective employees, officers and agencies.

26. INSURANCE SCHEDULE. Unless expressly waived in writing by the Lead State or Participating States, Contractor, as an independent contractor and not an employee of the Lead State or Participating States, must carry policies of insurance in amounts specified in this Insurance Schedule and/or any Insurance Schedule agreed by Contractor and a Participating State via a participating addendum, and pay all taxes and fees incident hereunto. The Lead State and Participating States shall have no liability except as specifically provided in the Contract. The Contractor shall not commence work before:

1) Contractor has provided the required evidence of insurance to the Lead State.

The Lead State's approval of any changes to insurance coverage during the course of performance shall constitute an ongoing condition subsequent this Contract. Any failure of the Lead State to timely approve shall not constitute a waiver of the condition.

Insurance Coverage: The Contractor shall, at the Contractor's sole expense, procure, maintain and keep in force for the duration of the Contract the following insurance conforming to the minimum requirements specified below. Unless specifically stated herein or otherwise agreed to by the Lead State, the required insurance shall be in effect prior to the commencement of work by the Contractor and shall continue in force as appropriate until the latter of:

1. Final acceptance by the Lead State of the completion of this Contract; or
2. Such time as the insurance is no longer required by the Lead State under the terms of this Contract.

Any insurance or self-insurance available to the Lead State shall be excess of and non-contributing with any insurance required from Contractor. Contractor's required insurance policies shall apply on a primary basis. Until such time as the insurance is no longer required by the Lead State, Contractor shall provide the Lead State with renewal or replacement evidence of insurance no less than thirty (30) days before the expiration or replacement of the required insurance. If at any time during the period when insurance is required by the Contract, an insurer or surety shall fail to comply with the requirements of this Contract, as soon as Contractor has knowledge of any such failure, Contractor shall immediately notify the State and immediately replace such insurance or bond with an insurer meeting the requirements. Contractor agrees that the following insurance coverages and policy limits shall also apply to, and operate for the benefit of, each Participating Entity that participates in this Contract pursuant to a Participating Entity.

Workers' Compensation and Employer's Liability Insurance

1) Contractor shall provide proof of worker's compensation insurance.
2) Employer's Liability insurance with a minimum limit of $500,000 each employee per accident for bodily injury by accident or disease.

Commercial General Liability Insurance

1) Minimum Limits required:

$25,000,000.00 General Aggregate
$25,000,000.00 Products & Completed Operations Aggregate
$5,000,000.00 Personal and Advertising Injury
$5,000,000.00 Each Occurrence

2) Coverage shall be on an occurrence basis and shall be at least as broad as ISO form CG 00 01 (or a substitute form providing equivalent coverage); and shall cover liability arising from premises, operations, independent contractors, completed operations, personal injury, products, civil lawsuits, Title VII actions and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).

Business Automobile Liability Insurance

1) Minimum Limit required: **$Waived** Each Occurrence for bodily injury and property damage.
2) Coverage shall be for "any auto" (including owned, non-owned and hired vehicles). The policy shall be written on ISO form CA 00 01 or a substitute providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage.

Professional Liability Insurance

1) Minimum Limit required: $ **Waived** Each Claim
2) Retroactive date: Prior to commencement of the performance of the Contract
3) Discovery period: Three (3) years after termination date of Contract.
4) A certified copy of this policy may be required.

Umbrella or Excess Liability Insurance

1) May be used to achieve the above minimum liability limits.
2) Shall be endorsed to state it is "As Broad as Primary Policy"

Commercial Crime Insurance

Minimum Limit required: **$Waived** Per Loss for Employee Dishonesty
This insurance shall be underwritten on a blanket form amending the definition of "employee" to include all employees of the Vendor regardless of position or category.

General Requirements:

b. Waiver of Subrogation: Each liability insurance policy shall provide for a waiver of subrogation as to additional insureds.

c. Cross-Liability: All required liability policies shall provide cross-liability coverage as would be achieve under the standard ISO separation of insureds clause.

d. Deductibles and Self-Insured Retentions: Any deductible or self-insured retention shall be at the sole risk of the Contractor.

e. Policy Cancellation: Except for ten (10) days notice for non-payment of premium, each insurance policy shall be endorsed to state that; without thirty (30) days prior written notice to the Lead State, the policy shall not be canceled or non-renewed, and shall provide that notices required by this paragraph shall be sent by mail to the address identified on page 1 of the Contract.

f. Approved Insurer: Each insurance policy shall be:

1) Issued by insurance companies authorized to do business in the Lead State and Participating States or eligible surplus lines insurers acceptable to the Lead State and Participating States and having agents upon whom service of process may be made, and

2) Currently rated by A.M. Best as "A-VII" or better.

Evidence of Insurance:

Prior to the start of any Work, Contractor must provide the following documents to the Lead State:
1) Certificate of Insurance: The Acord 25 Certificate of Insurance form or a form substantially similar must be submitted to the State to evidence the insurance policies and coverages required of Contractor.
2) Schedule of Underlying Insurance Policies: If Umbrella or Excess policy is evidenced to comply with minimum limits, a copy of the Underlyer Schedule from the Umbrella or Excess insurance policy may be required.

Review and Approval: Documents specified above must be submitted for review and approval by the Lead State prior to the commencement of work by Contractor. Neither approval by the Lead State nor failure to disapprove the insurance furnished by Contractor shall relieve Contractor of Contractor's full responsibility to provide the insurance required by this Contract. Compliance with the insurance requirements of this Contract shall not limit the liability of Contractor or its sub-contractors, employees or agents to the Lead State or others, and shall be in addition to and not in lieu of any other remedy available to the Lead State or Participating States under this Contract or otherwise.

Mail all required insurance documents to the Lead State identified on page one of the Contract

27. COMPLIANCE WITH LEGAL OBLIGATIONS. Any and all supplies, services and equipment bid and furnished shall comply fully with all applicable Federal and State laws and regulations. Contractor shall procure and maintain for the duration of this Contract any state, county, city or federal license, authorization, waiver, permit, qualification or certification required by statute, ordinance, law, or regulation to be held by Contractor to provide the goods or services required by this Contract.

28. WAIVER OF BREACH. Failure to declare a breach or the actual waiver of any particular breach of the Contract or its material or nonmaterial terms by either party shall not operate as a waiver by such party of any of its rights or remedies as to any other breach.

29. SEVERABILITY. If any provision of this Contract is declared by a court to be illegal or in conflict with any law, the validity of the remaining terms and provisions shall not be affected; and the rights and obligations of the parties shall be construed and enforced as if the Contract did not contain the particular provision held to be invalid.

30. ASSIGNMENT/DELEGATION. To the extent that any assignment of any right under this Contract changes the duty of either party, increases the burden or risk involved, impairs the chances of obtaining the performance of this Contract, attempts to operate as a novation, or includes a waiver or abrogation of any defense to payment by State, such offending portion of the assignment shall be void, and shall be a breach of this Contract. Contractor shall not assign, sell, transfer, subcontract or sublet rights, or

delegate responsibilities under this Contract, in whole or in part, without the prior written approval of the WSCA Contract Administrator, which approval shall not be unreasonably withheld.

31. **OWNERSHIP OF PROPRIETARY INFORMATION.** Any reports, histories, studies, tests, manuals, instructions, photographs, negatives, blue prints, plans, maps, data, system designs, computer code, or any other documents or drawings, prepared or in the course of preparation by Contractor (or its subcontractors) specifically for WSCA in performance of Contractor's obligations under this Contract (collectively, the "Specially Prepared Proprietary Information") shall be the exclusive property of WSCA and all such Specially Prepared Proprietary Information, that has not already been delivered into WSCA's possession, shall be delivered into WSCA possession by Contractor upon completion, termination, or cancellation of this Contract. For purposes of this delivery obligation, Contractor shall provide the Specially Prepared Information to the Lead State. Contractor shall not use, willingly allow, or cause to have such Specially Prepared Information used for any purpose other than performance of Contractor's obligations under this Contract without the prior written consent of WSCA. Notwithstanding the foregoing, unless otherwise specifically stated in the Contract, neither WSCA nor any Participating Entities shall have any proprietary interest in any reports, histories, studies, tests, manuals, instructions, photographs, negatives, blue prints, plans, maps, data, system designs, computer code, or any other documents or drawings, any pre-existing works or materials, or any materials licensed to WSCA (or otherwise provided for WSCA's use) that are NOT specifically prepared by Contractor for WSCA in performance of Contractor's obligations under this Contract, whether such materials are subject to patent, trademark or copyright protection or otherwise.

32. **PATENTS, COPYRIGHTS, ETC.** The Contractor shall release, indemnify and hold WSCA, the Lead State, and Participating States and their officers, agents and employees harmless from liability of any kind or nature, including the Contractor's use of any copyrighted or un-copyrighted composition, secret process, patented or unpatented invention, article or appliance furnished or used in the performance of this Contract.

33. **PUBLIC RECORDS.** Pursuant to NRS 239.010, information or documents received from Contractor may be open to public inspection and copying. The Lead State will have the duty to disclose unless a particular record is made confidential by law or a common law balancing of interests. Contractor may label specific parts of an individual document as a "trade secret" or "confidential" in accordance with NRS 333.333, provided that Contractor thereby agrees to indemnify and defend the Lead State for honoring such a designation. The failure to so label any document that is released by the Lead State shall constitute a complete waiver of any and all claims for damages caused by any release of the records.

The above provision applies to WSCA and the Lead State, and does not inure to the benefit of Participating Entities. Information or documents produced or received by a Participating Entity in connection with participation in this Contract shall be subject to the public records laws of the Participating Entity's state, ,and the provisions of the applicable Participating Addendum.

34. **CONFIDENTIALITY.** Contractor shall comply with applicable laws with respect to confidentiality of all information, in whatever form, produced, prepared, observed or received by

Contractor in connection with the Contract. Unless otherwise mandated by court order, or unless otherwise required by applicable law, Contractor shall keep confidential all information observed or received by Contractor in connection with the Contract to the extent that such information is made confidential under the terms of this Contract.

35. **NONDISCRIMINATION.** Contractor agrees to abide by the provisions of Title VI and Title VII of the Civil Rights Act of 1964 (42 USC 2000e), which prohibit discrimination against any employee or applicant for employment, or any applicant or recipient of services, on the basis of race, religion, color, or national origin; and further agrees to abide by Executive Order No. 11246, as amended, which prohibits discrimination on basis of sex; 45 CFR 90 which prohibits discrimination on the basis of age, and Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities. Contractor further agrees to furnish information and reports to requesting Participating Entities, upon request, for the purpose of determining compliance with these statutes. Contractor agrees to comply with each individual Participating State's certification requirements, if any, as stated in the special terms and conditions. This Contract may be canceled if the Contractor fails to comply with the provisions of these laws and regulations. Contractor must include this provision in very subcontract relating to purchases by the States to insure that subcontractors and vendors are bound by this provision.

36. **FEDERAL FUNDING.** In the event federal funds are used for payment of all or part of this Contract:

a. Contractor certifies, by signing this Contract, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any federal department or agency. This certification is made pursuant to the regulations implementing Executive Order 12549, Debarment and Suspension, 28 C.F.R. pt. 67, §67.510, as published as pt. VII of the May 26, 1988, Federal Register (pp. 19160-19211), and any relevant program-specific regulations. This provision shall be required of every subcontractor receiving any payment in whole or in part from federal funds.

b. Contractor and its subcontractors shall comply with all terms, conditions, and requirements of the Americans with Disabilities Act of 1990 (P.L. 101-136), 42 U.S.C. 12101, as amended, and regulations adopted thereunder contained in 28 C.F.R. 26.101-36.999, inclusive, and any relevant program-specific regulations.

c. Contractor and its subcontractors shall comply with the requirements of the Civil Rights Act of 1964, as amended, the Rehabilitation Act of 1973, P.L. 93-112, as amended, and any relevant program-specific regulations, and shall not discriminate against any employee or offeror for employment because of race, national origin, creed, color, sex, religion, age, disability or handicap condition (including AIDS and AIDS-related conditions.)

37. **LOBBYING.** The parties agree, whether expressly prohibited by federal law, or otherwise, that no funding associated with this Contract will be used for any purpose associated with or related to lobbying or influencing or attempting to lobby or influence for any purpose the following:

a. Any federal, state, county or local agency, legislature, commission, counsel or board;

b. Any federal, state, county or local legislator, commission member, counsel member, board member, or other elected official; or

c. Any officer or employee of any federal, state, county or local agency; legislature, commission, counsel or board.

38. **NON-COLLUSION.** Contractor certifies that this Contract and the underlying bid, have been arrived at independently and have been without collusion with, and without any agreement, understanding or planned common course of action with, any other vendor of materials, supplies, equipment or services described in the invitation to bid, designed to limit independent bidding or competition.

39. **WARRANTIES.** Contractor warrants that all services, deliverables, and/or work product under this Contract shall be completed in a workmanlike manner consistent with standards in the trade, profession, or industry. Except as specifically set forth above, Contractor makes no representations or warranties, express or implied, and specifically disclaims any representation or warranty of merchantability, fitness for a particular purpose, title, non-infringement or any warranty arising by usage of trade or course of dealing. Further, Contractor makes no representation or warranty that wireless calls or other transmissions will be routed or completed without error or interruption (including calls to 911 or any similar emergency response number), or guarantee regarding network security, the encryption employed by any service, the integrity of any data that is sent, backed up, stored or subject to load balancing, or that contractor's security procedures will prevent the loss or alteration of, or improper access to, a Participating Entity's data and information. Contractor does not authorize anyone to make a warranty of any kind on its behalf, and Participating Entities should not rely on anyone making such statements. Contractor is not the manufacturer of equipment purchased by or provided to participating entities in connection with use of the service.

40. **CONFLICT OF INTEREST.** Contractor certifies that it has not offered or given any gift or compensation prohibited by the state laws of any WSCA Participating Entities to any officer or employee of WSCA or Participating Entities to secure favorable treatment with respect to being awarded this Contract.

41. **INDEPENDENT CONTRACTOR.** Contractor shall be an independent contractor, and as such shall have no authorization, express or implied to bind WSCA or the respective Participating Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to perform any acts as agent for WSCA or the Participating Entities, except as expressly set forth herein.

42. POLITICAL SUBDIVISION PARTICIPATION. Participation under this Contract by authorized political subdivisions shall be voluntarily determined by the corresponding political subdivision. Contractor agrees to provide products and services to such political subdivisions based upon the same terms, conditions and prices set forth in the corresponding Participating Addendum.

43. PROPER AUTHORITY. The parties hereto represent and warrant that the person executing this Contract, a Participating Addendum, and/or order, as applicable, on behalf of the corresponding party has full power and authority to do so. Contractor acknowledges that as required by statute or regulation the Contract is effective only after approval by the WSCA Board of Directors and only for the period of time specified in the Contract. Except as otherwise provided herein, any services performed by Contractor before this Contract is effective or after it ceases to be effective are performed at the sole risk of Contractor. The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency.

44. GOVERNING LAW; JURISDICTION.

44.1 Lead State. The parties acknowledge and agree that with respect to Contractor and the Lead State and/or WSCA, the rights and obligations of the parties hereto shall be governed and construed in accordance with the laws of the state of Nevada, without giving effect to any principle of conflict-of-law that would require the application of the law of any other jurisdiction. The parties consent to the exclusive jurisdiction of the First Judicial District Court, Carson City, Nevada for enforcement of this Contract.

44.2 Participating Entities. The construction and effect of any Participating Addendum or order against the Contract shall be governed by and construed in accordance with the laws of the corresponding Participating Entity. Venue for any claim, dispute or action concerning an order placed against the Contract or the effect of a Participating Addendum shall be in the Participating Entity's State.

45. SIGNATURES IN COUNTERPART. The Contract may be signed in any number of counterparts, each of which shall be an original, but all of which together shall constitute one in the same instrument.

46. AMENDMENTS. The terms of this Contract shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the WSCA Contract administrator. Each Participating Entity expressly acknowledge and agree that it will be bound by the terms and conditions of the Contract and by all existing or future amendments or modifications thereto, all of which are incorporated herein by reference, without the necessity of further action or notice by Contractor or the Lead State. Each Participating Entity hereby consents to and waives notice of any such amendments and modifications.

47. ENTIRE CONTRACT. This Contract, its integrated attachment(s) and, the Participating Addenda, as applicable constitute the entire agreement of the parties and such are intended as a complete

terms and conditions of the Contract and by all existing or future amendments or modifications thereto, all of which are incorporated herein by reference, without the necessity of further action or notice by Contractor or the Lead State. Each Participating Entity hereby consents to and waives notice of any such amendments and modifications.

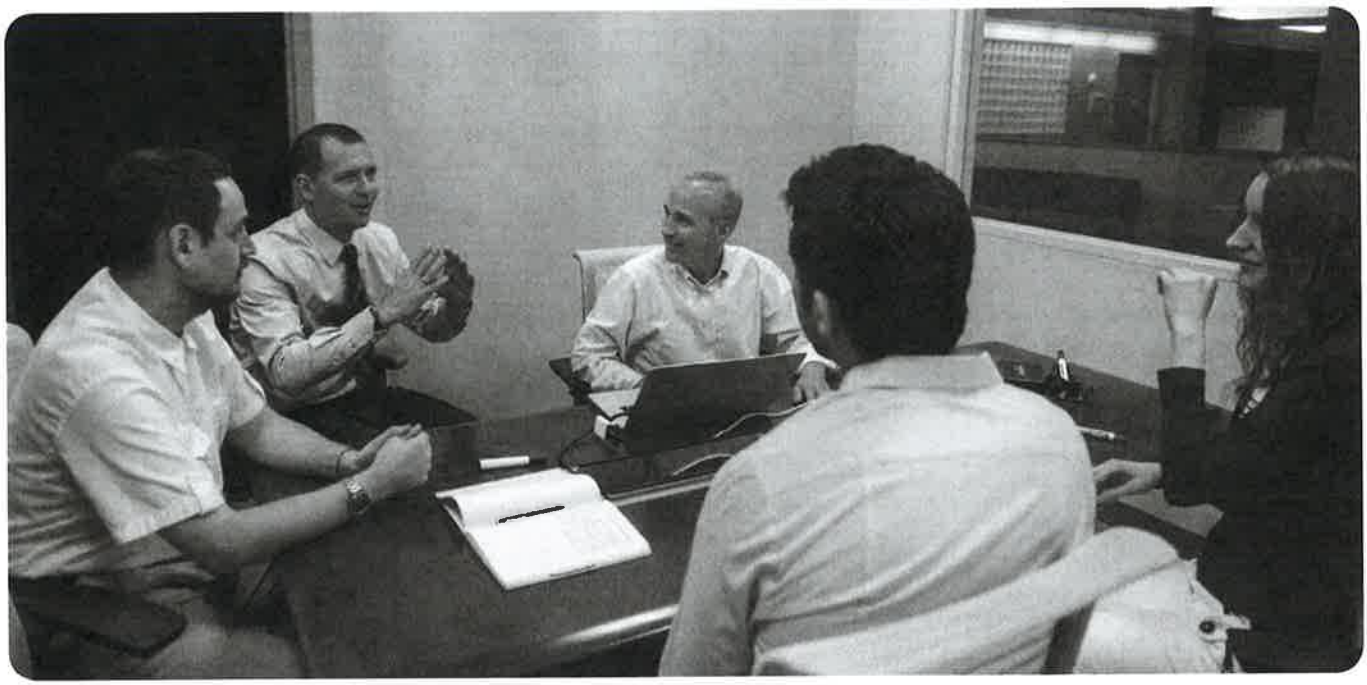
47. **ENTIRE CONTRACT.** This Contract, its integrated attachment(s) and, the Participating Addenda, as applicable constitute the entire agreement of the parties and such are intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof.

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be signed and intend to be legally bound thereby.

Independent Contractor's Signature	Date AT.T Independent's Contractor's Title
Signature	Date Director of Contracts Title
Greg Smith, Administrator, State of Nevada	APPROVED BY WSCA DIRECTORS
On 3-14-12 (Date)	On _____ (Date)

Approved as to form by:

Deputy Attorney General for Attorney General	On 14 March 12 (Date)



Business Continuity Preparedness Handbook

Managing risk through proactive planning

June 2016

Table of contents

Executive summary	2
AT&T alignment with industry standards	3
AT&T business continuity management	6
AT&T network disaster recovery capabilities	7
Business continuity preparedness — best practices	8
Planning is essential	10
Solutions for business continuity strategies	11
AT&T business solutions portfolio	12
Collaboration – unified communications	13
Collaboration – messaging	15
Remote access services/mobility	16
Contact center	18
Hosting & application management	19
AT&T enterprise recovery services	21
Managing network security	22
AT&T customer support	24
Additional information	26

With growing concern over extreme weather conditions and national security breaches, it's essential to take a proactive approach to business continuity planning to help minimize the impact of an event to customers, employees and stakeholders. Developing and testing a plan that protects the health and safety of employees and maintains critical business functions requires a comprehensive cross-organizational effort.

Executive summary

When it comes to business continuity, proactive planning and a strong execution strategy are essential steps in reducing exposure from any type of "event", natural or man-made, accidental or intentional, internal or external, with or without prior warning. AT&T has developed this business continuity preparedness handbook to provide an overview of best practices that can help facilitate proactive planning and ongoing enforcement for all event scenarios. It also provides a business continuity preparedness self-assessment to help organizations identify potential gaps in their preparedness planning. As illustrated by the AT&T business continuity survey results included in this handbook, with the ongoing evolution of technology and cyber threats, it is critical for organizations to maintain operational effectiveness and flexibility for any scenario-regardless of cause or duration.

This handbook covers the following topics:

- AT&T alignment with industry standards
- AT&T business continuity survey results
- AT&T business continuity management practices
- Business continuity preparedness-best practices
- Solutions for business continuity strategies
- AT&T customer support during an event
- Additional resources

AT&T alignment with industry standards

In 2015, AT&T became the first telecom service provider to be certified under the new international Business Continuity Management standard (ISO 22301:2012) for the Voluntary Private Sector Preparedness Program (PS-Prep™). The new ISO standard is the logical successor to the previous standard and became the accepted Business Continuity Management standard worldwide. This PS-Prep™ re-certification demonstrates that AT&T continues to be equipped to resume business operations and continue delivering services to its customers in the vital hours and days after a disaster strikes. In the event of any disaster or other emergency, we will be able to quickly resume network traffic, field customer calls and queries, and service the communities in which we operate. PS-Prep™ is a partnership between the Department of Homeland Security and the private sector enabling private businesses to demonstrate their capabilities for planning for, responding to, and recovering from disasters and other emergencies. We received our original certification for PS-Prep in 2012.

In addition to ISO 22301, the business continuity management program also is:

- Certified by CTIA as part of their Business Continuity/ Disaster Recovery Program since 2004
- Aligned with the Disaster Recovery Institute International (DRII) Professional Practices since 2004
- Aligned with the National Incident Management System (NIMS) as suggested by the Department of Homeland Security (DHS) since 2004
- ISO 27001 certified for information security since 2010
- Aligned with the BCI Good Practice Guidelines since 2011

PS-Prep™ – Certified –

ISO 22301:2012

"Our customers rely on us for 24x7 connectivity especially during times of natural disasters where we provide a critical lifeline. So we're proud to be the first telecom to secure re-certification under the new ISO standard. This recognition demonstrates once again that our business continuity program, coupled with our technology recovery team, is best in class."

— John Donovan, Senior Executive Vice President, AT&T Technology and Operations

AT&T business continuity survey results

AT&T business continuity survey results show fears of potential security breaches and natural disasters, including extreme weather conditions, weighing heavily on IT executives, businesses nationwide have continued to grow and advance their business continuity and disaster recovery plans to incorporate the adoption of wireless network capabilities, cloud services and mobile applications.

The results for the latest AT&T annual business continuity study identify several trends regarding how businesses are preparing themselves for potential disasters and threats. AT&T has conducted this study for thirteen consecutive years, surveying IT executives from companies in the United States with at least $25 million in annual revenue, to measure the national pulse on business continuity planning. Our business continuity study is based on a sample of 500 online surveys among Information Technology (IT) executives with primary responsibility for business continuity planning, 59% of them representing companies with locations outside the U.S. The study was conducted by Research Now with respondent geographic representation as follows:

- 28% in the Northeast
- 25% in the South
- 20% in the Midwest
- 27% in the West

The following highlights some of our key findings from the study:

- Executives increasingly consider managing security requirements specific to mobile deployment (51%) and cloud (48%) as important business concerns.
- 54% of executives indicate that IT budgets have increased over the past two years, with "increasing data security" (31%) as one of the leading motivations for investing in new technologies.
- In order to respond to these growing concerns, businesses are investing in highly secure platforms across the entire IT landscape, with companies most frequently investing in cloud services (39%) and mobile applications (35%), followed closely by network security solutions (33%).

"We're seeing more and more major security events dramatically impact business operations across virtually every industry."

— Jason Porter, Vice President, Security Solutions, AT&T Business Solutions

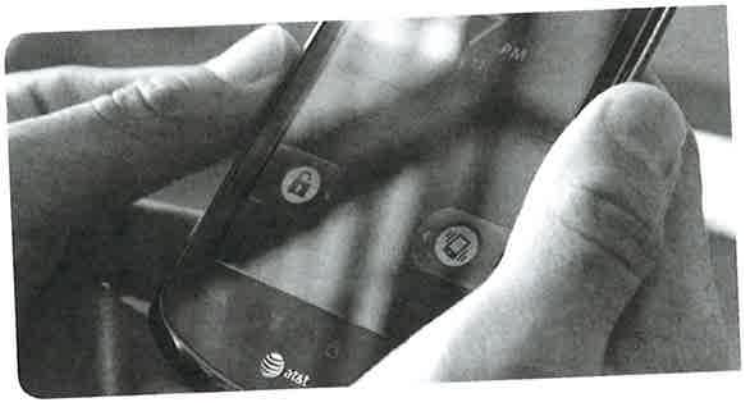
Our business continuity study key findings

As devices infiltrate the workforce and organizations expand globally, companies are looking beyond the impact of natural disasters when evaluating their business continuity strategies. They are now evaluating the ongoing impact of security breaches and the tools needed to not only to mitigate risks but also proactively anticipate potential internal and external threats to their organizations.

- 81% of companies indicate that their business continuity plan accommodates the possibility of a network security event, such as malware, phishing, bugs and malicious hackers.
- 63% of business leaders classify security breaches as their number one business concern in relation to overall security strategies.

Although the majority of companies (89%) indicate that they have a proactive approach to overall security, less than half of those polled (49%) claim they have a strong execution strategy in place. The AT&T survey found that although business leaders have the right tools in place, the amount of threats infiltrating the business now require stronger requirements on the front and back end to fend off ongoing attacks.

- 86% of companies surveyed are concerned about the use of mobile networks and devices.
- Over one-third (34%) have experienced a distributed denial-of-service (DDoS) attack in the past 24 months. However, only half of organizations (50%) are currently taking proactive measures against protecting their company against DDoS attacks.
- Similarly, one-fourth (26%) of companies have experienced an advanced persistent threat (APT) attack in the past 24 months. However, only 44% of respondents are taking a proactive approach to protecting their companies against advanced persistent threats.



AT&T business continuity management

Planning for and responding to crises is something that we perform without hesitation and with extensive experience in a wide variety of situations, from hurricanes to floods, to power outages, work stoppage contingency planning, and man-made disasters. We have a global team of experts who practice this response several times per year. Our business continuity efforts include: the day-to-day operational activities required to maintain continued service to its customers, broad scenario planning as well as individual threat assessment and analysis, centralized command and control responsibility and specific recovery procedures for key business processes. We take appropriate actions for the delivery of services to customers while considering and addressing the needs of our employees and their families.

"When an event occurs, our top priority is to account for our employees and to assess their personal impacts. This allows our employees to then focus on our customers' needs."

– Lisa Tenorio, AT&T Assistant VP, Corporate Business Continuity Planning

AT&T has a team of industry-leading, certified and experienced business continuity experts engaged in the AT&T internal business continuity management program to achieve its business objectives. This team requires that key business processes have documented business continuity plans that are updated and exercised on a predetermined schedule. Plan exercises are designed around specific scenarios to test the viability and capability of the plans. Plan development and plan exercise execution are based on the concept of continuous improvement with the focus of maintaining business operations. As part of that planning, AT&T has performed an extensive corporate-wide risk assessment, and implemented incident response and contingency planning on several broad fronts:

Employees and facilities

It is the policy of AT&T to provision and maintain products and services in an environmentally responsible and sustainable manner. The company implements strategies based on best practices to reduce risk and to help mitigate operational impacts during an event. During events, AT&T extensively utilizes text messaging and notification tools to notify employees and our first responder teams; sharing status and providing local resources to impacted employees to assist with their personal recovery needs.

Business process

We design our services to help our key business processes remain operational and keep customer service impacts to a minimum. Through a comprehensive response, recovery, and restoration program, AT&T helps support reliability of its key business processes and infrastructures.

Supplier BCP

AT&T promotes supplier business continuity capabilities that are aligned with our business requirements. Suppliers providing products and services supporting AT&T business activities are documented in the business unit's business continuity plan. Suppliers supporting essential business activities are requested to complete a BCP Survey based on a pre-defined schedule identifying whether a business continuity program is in place. For more information, visit *Doing Business with Us* on the Web (att.com/dbw).

Network infrastructure

In the event of a disaster, as customers implement their own business continuity plans, a shift in traffic patterns on the AT&T Global Network may result. AT&T proactively plans for these shifts in wireless and wireline voice and data traffic patterns evaluating alternatives to maximize network performance.

Information Technology Service Continuity

The AT&T Information Technology Service Continuity (ITSC) Program is committed to identifying and managing IT-related service continuity risks across the enterprise. The organization has established safeguards to minimize the risk, cost, and duration of disruption to key business processes in the event of a crisis or disaster. Accordingly, ITSC has taken a number of steps to increase the reliability of AT&T key business processes and supporting infrastructures in order to provide high-quality communication services to AT&T customers. This includes prevention and mitigation efforts, as well as comprehensive emergency response and recovery plans in the event of a disaster or crisis.

Information/cyber security

The AT&T chief security office (CSO) establishes policies and requirements, as well as comprehensive programs, to incorporate security into all facets of computing and networking environments. The AT&T security program implements the AT&T security policies through a rich set of initiatives, processes and procedures administered by the AT&T security organization worldwide and certified to the ISO/IEC 27001:2005 Information Security Management Standard. These program initiatives are executed on an ongoing basis by each region and are supported by the global network security teams. The goal of the program is to protect both AT&T and each customer's information and resources.

AT&T community support

When disaster strikes, we are ready to provide meaningful humanitarian assistance to residents and first responders. Together with relief organizations and community volunteers, our people and resources can make a difference and provide critical support to those in need. We're proud to serve our communities by making critical connections in good times and bad.

Our network disaster recovery capabilities

AT&T developed its network disaster recovery (NDR) capability specifically to allow rapid service recovery following the catastrophic loss of a network office. Network disaster recovery provides business continuity and recovery capabilities for the AT&T Global Network. AT&T has invested more than 600 million dollars in its NDR program since its inception in 1991; our dedicated recovery fleet now has more than 320 trailers and support vehicles. One of the primary roles of the network disaster recovery organization is to recover the services of an AT&T network office that has been completely destroyed or compromised by a natural or man-made disaster. This type of restoration would exceed the normal capabilities of the AT&T network operations maintenance processes and would require the long-term deployment of specialized equipment and resources.

The AT&T NDR Team includes AT&T managers, engineers and technicians who have received special training in the physical recovery of the AT&T network. Members participate in several recovery exercises each year to sharpen and practice their skills using NDR's disaster recovery equipment and processes. The exercises test as many of the NDR processes as possible, from the initial team call-out, to equipment transportation and set-up, to technology turn-up and testing. NDR has conducted three or four technology recovery exercises in the field each year since the program's formation. The NDR Team includes members who have been trained as hazardous materials technicians. This training allows them to perform assessment, recovery and maintenance activities in contaminated environments while wearing specialized personal protective equipment.

- NDR's recovery equipment includes a fleet of specially-designed semi-tractor trailers that contain the same type of equipment that is normally installed in permanent AT&T offices. These technology trailers can be interconnected to recover the capabilities of a network office that has been heavily damaged or destroyed. The equipment is maintained in and deployed from warehouses strategically located in the U.S. and abroad.
- NDR establishes broadband and wireless voice and data connectivity from disaster sites using one or more Emergency Communications Vehicles (ECV). An ECV uses a satellite link to provide NDR with command communications during the initial phase of a recovery effort. The ECVs have also been used to provide command and humanitarian relief communications capability to other emergency responders.
- AT&T uses Cells on Wheels (COWs) and Cells on Light Trucks (COLTs), self-contained mobile cell sites, to provide extra cellular capacity to restore communications after a disaster. The mobile sites can be used to replace the service of a failed permanent cell site and they can be used to supplement the cellular capacity of an area that has increased demand. The NDR Team uses Satellite COWs and COLTs to establish first-in communications when terrestrial connections to the AT&T Network are not immediately available.

Assess your own level of preparedness with the following questions

Mitigate risk, protect mission - critical resources

- ☐ Has the organization assessed the impact of a potential disruption?
- ☐ Has the organization analyzed which business processes, applications, facilities, suppliers, workgroups, or vital records are most critical?
- ☐ Has the organization created a strategy to recover from potential impacts? Are new scenarios, threats, and vulnerabilities addressed in your planning process?
- ☐ Has the organization developed and exercised a business continuity plan to mitigate business risk?
- ☐ Is this plan maintained and reviewed with the organization's response team on a regular basis?
- ☐ Is the plan approved by organization leadership?
- ☐ Are key locations hardened and facilities conditioned?
- ☐ What physical and logical security measures are in place?
- ☐ Do the security measures in place also address potential exposure from cloud and mobile technology?

Meet regulatory requirements and customer service level agreements

- ☐ Does the organization or its business partners have regulatory mandated performance or availability service levels?
- ☐ Has the organization complied with all current or regulatory requirements or public policy mandates?

Invest wisely

- ☐ Has the organization quantified the potential costs of downtime or total business failure?
- ☐ Has the organization developed sound business cases to optimally invest in risk mitigation?

- The NDR fleet includes eight mobile command centers. The trailers can be rapidly deployed and set up within an hour of arriving at a recovery site. The command centers have data and voice communications capabilities (provided by the ECVs) and provide NDR's incident command team with a fully-equipped and controlled office space during disaster responses. For large and/or long-term responses, a base camp can be established that will provide AT&T responders with access to a full kitchen, a dining facility and sleeping quarters. AT&T has a large inventory of MREs (meals ready to eat) and other supplies set aside for use during emergency responses.

Business continuity preparedness — best practices

All companies and government agencies, regardless of size, need to identify their mission-critical business processes and effectively manage the risks around them, whether from a pandemic, hurricane, earthquake or any other kind of crisis. Mission-critical business processes are those that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public, or sustain its industrial or economic base. In addition, the complexities of maintaining mobility and wireless capabilities during a disaster or security threat has become increasingly important for businesses as they consider business continuity planning. Taking a proactive approach to business continuity is essential for being prepared to respond when disaster strikes. Plans should specify redundant systems, back-up sites, employee communications, and alternative work sites. They also should include a process for maintaining customer service, and customer communications immediately following the crisis and proceeding until things return to normal. Business Continuity Management, involves business sustainability through a period of significant interruption caused by a disaster or any other disruptive event. An unplanned interruption could have an impact on national security, citizen services and economic well-being.

Business Continuity Management is good business practice because it enables organizations to continue their essential functions across a broad spectrum of hazards and emergencies. It is essential for all types of scenarios ranging from system or component failure caused by a software upgrade to a man-made or natural disaster that broadly impacts an organization's physical assets, buildings and/or people. Following is a set of key planning principles that apply to business continuity scenarios in the public or private sector.

The following outlines six key steps in preparing for any type of business continuity process. The more accurate an organization can be in its planning, the more prepared it will be in the long run.

Identify key business processes and impacts

The first step is to understand what processes are critical to the business and how different disaster scenarios could impact continuity of operations. For example, how could demand for products and services be affected – will it grow or decline? What is the impact to the organization in terms of leadership, capabilities, security and communications, and what does that mean for the operation of mission-critical functions? The answers to these types of questions could determine the type of response required. This step is vital so that, with delegation of authority or orders of succession established, attention and resources can effectively focus on a rapid response to the situation.

Perform risk assessment, risk treatment and management

To continue with key business processes in a crisis, it is necessary for an organization to complete a functional risk assessment to help address the essential functions first and make the appropriate investments, in time and money. The risk assessment will identify the processes, resources and suppliers which would have the greatest impact on a company's ability to serve its customers or an agency's ability to achieve its mission objectives. It also involves the identification and assessment of the potential threats, the existing vulnerabilities and the probability that a threat will exploit the identified vulnerabilities. This aids in the identification of risk exposure to different components of the organization, so that fact-based decision making on mitigation plans can occur.

Determine recovery strategies

The next step is to define the organization's business continuity strategies. For example, how does the organization want its business to perform and what options are available? Does the organization keep the same service level agreements or does it prioritize work? In addition, alternate facilities and their desirable characteristics must be considered. The results of the risk assessment and the identification of recovery strategies are instrumental in the development of continuity plans to address specific threats.

It is also critical that these activities be accomplished in a methodical and consistent way across the organization so that all parts of the business are preparing for the same scenarios, using the same information to certify that the end-to-end plans are effective.

Develop business continuity/disaster recovery (BC/DR) plans and provision DR capabilities

Continuity plans should be developed to provide interoperable communication and continuity of key business operations with essential suppliers, or other agencies, until normal operation can be resumed. Delegation of Authority and Orders of Succession support that businesses plan for the loss of leadership so that essential business operations could continue if key executives are incapacitated. Continuity plans should identify not only incremental strategic or procedural changes, but also any gaps in capabilities that need to be addressed. It is important to implement any new capabilities prior to the event occurring, to allow a business to successfully recover at time of disaster.

Train, test and exercise

Emergency response team members need to be provided opportunities to acquire the skills to perform their assigned business continuity roles. Business continuity plans must be capable of implementation with or without warning. They must be tested on a regular basis and in as real a way as possible to validate their effectiveness when a disaster occurs. This requires the development of a test plan, detailing how a business will test capabilities, as well as an emergency response guidebook. In addition to conducting simulation exercises, recovery strategy implementations are necessary to validate operational effectiveness.

Monitor and improve performance

Situations evolve over time and are not static. An organization should consider how changes to a situation and the business environment could affect preparedness. To validate that a plan works at the time of a disaster, business continuity plans should be considered an organizational priority and reviewed regularly. In addition, changes to normal operations must also be reflected in business continuity plans and the emergency response guidebook, whether they are system upgrades, process changes or resource restructuring.

Planning is essential

When a disaster strikes, an organization's ability to respond quickly and effectively may be critical in protecting its staff, profits, reputation and essential operations. Developing a plan that protects the health and safety of employees and maintains key business processes requires a comprehensive and cross-organizational planning effort.

Review and expand existing business continuity plans to include the landscape of threats over larger geographic regions

While many organizations have business continuity plans to deal with regional events, they may not be prepared for an event that could occur on a global scale. Existing business continuity plans should be reviewed and supplemented accordingly to meet the needs of a range of threats.

Utilize credible sources

It's important to identify reliable and credible sources of information early on in the planning process and to track developments.

Develop planning phases with trigger points

Organizations should create clearly defined response-planning phases with trigger points for moving from one phase to another. For example, resources such as the Federal Emergency Management Agency (FEMA) can be used as a reference point for disaster and event planning. Similarly, the World Health Organization (WHO) has developed a planning checklist for large businesses that can be used as a reference point for defining phases and trigger points for proactive planning activities.

Build escalating scenarios and perform simulation exercises to identify gaps

Many organizations are conducting business continuity planning exercises using a range of scenarios to assess the impact of a disaster on their businesses. For example, they may have one scenario designed to simulate a local flood and a second that assesses the impact of a Category F5 Tornado impacting several locations simultaneously. Scenario-based exercises help identify gaps and risks that might not otherwise be obvious. Build scenarios starting with a small event and then move up to one with potential for significant impact.

Communication is crucial

The ability of an organization to withstand a crisis may ultimately rest on the effectiveness of its communications with employees, customers, suppliers and other key interested parties. Senior executives should be ready to deliver the right messages both internally and externally.

Network solutions for business continuity preparedness require advanced planning and implementation to effectively enable survivability of a firm's critical operations

Organizations should be prepared to respond to additional demands that might result from their continuity plans, such as increased virtual office work and associated increased demand on their Virtual Private Network (VPN). These concerns might include evaluating their current employee usage of the services, maximum expected increase in corporate infrastructure usage under different scenarios, increases in additional services required and employee preparedness for telecommuting. It is also prudent to provide employees who must work in a virtual office scenario with multiple options to access their corporate network.

AT&T offers a wide array of business continuity services

Solutions for business continuity strategies

An increasing number of organizations today are turning to experts for help with business continuity planning. Building on years of experience in managing and maintaining some of the world's largest and most complex networks (including its own), AT&T offers a wide array of business continuity services designed to provide customers with opportunities for continuous operation and availability of their key business processes, mission-critical applications, data, work centers and networks.

The AT&T National Security and Emergency Preparedness (NSEP) portfolio

Businesses who provide national security and emergency preparedness services can accomplish their critical missions under the most challenging natural and man-made circumstances with our continuing commitment to support a robust set of NSEP services.

In the event of crisis, AT&T has a resilient network with significant capacity that is complimented by robust operations to support NSEP services and NSEP users' needs.

AT&T offers a comprehensive suite of NSEP services, based on the following National Communications System (NCS) Programs:

- Telecommunications Service Priority (TSP)
- Government Emergency Telecommunications Service (GETS)
- Wireless Priority Service (WPS)

Further, AT&T is fully committed to providing robust NSEP services and to working closely with the NCS to develop next generation GETS over Internet Protocol (IP).

Telecommunications Service Priority

The Federal Communications Commission (FCC) established the TSP in 1988 to help determine what circuits should be restored and maintained first in a crisis. Telecommunication circuits most necessary for the nation's security and emergency preparedness functions are assigned TSP codes by the federal government and are given priority for restoration and installation. AT&T will give critical circuits with assigned TSP codes top priority for restoration, as required by the FCC.

TSP establishes the legal basis for Service Providers to act, when authorized by the FCC, on a priority basis in the provisioning and restoration of services supporting NSEP mission requirements. TSP is applicable to services such as dedicated private lines, access lines, dial-tone lines, high-capacity digital systems, and trunks between another carrier's switching or wireless nodes.

TSP is an FCC mandated program that is managed and administered by the Office of Emergency Communications (OEC). AT&T has a designated TSP Point of Contact (POC) to interact with the OEC. AT&T Customer Care Center supports TSP provisioning when orders are received from customers who are authorized by the FCC. Restoring service with TSP restoration priority is accomplished using special handling and escalation processes by the AT&T customer care specialists.

Government Emergency Telecommunications Service

GETS is a calling card service and is available to Federal, State, Local, and other Government authorized users.

GETS calls receive priority treatment in the network and have a high probability of completion when a disaster occurs or in situations that may result in network congestion.

Wireless Priority Service

AT&T Mobility supports NSEP critical users' needs for priority wireless call processing that can be enhanced when used with GETS priority treatment in the AT&T portfolio of NSEP services. AT&T Mobility manages all WPS related operations and administration in accordance with NCS guidelines.

WPS is offered on a subscription basis to Federal, State, Local and other Government authorized users. WPS users can dial the *272 feature code to queue for priority access to a radio traffic channel and network trunks. In cases where WPS calls terminate on a non-AT&T network; these calls can receive priority handling across the AT&T network.

Our business solutions portfolio

For organizations looking to update their business continuity plans, AT&T offers a wide array of business continuity services, encompassing disaster planning, risk management, recovery preparedness and communications readiness. In addition, services such as business impact analysis, risk assessments, enterprise hosting, cloud computing application services, and storage solutions, as well as high availability network solutions and network and IT security solutions can be important components of a company's business continuity plans.

The following pages provide information on some of the business solutions that AT&T can provide to support a customer's business continuity strategies. Each solution provides a synopsis of the Business Continuity/Disaster Recovery challenge and then how AT&T can help address that challenge. It is essential to design and implement these solutions before any type of potential business disruption occurs. Factors such as solution design time, provisioning cycle times and lead times for hardware procurement should all be planned for accordingly. All companies, regardless of size, need to identify their critical business components and effectively manage the risk around them, whether from a hurricane, an earthquake or any other kind of crisis. Unfortunately, many companies are still unprepared.

Collaboration – unified communications

Natural or man-made disasters can affect the ability of any company to communicate. As businesses implement their continuity plans, they may find they want to consider audio, Web and video conferencing and/or wireless video as part of their overall communications strategy for continued communications and operations as well as emergency response.

Business continuity/ disaster recovery challenge

During a disaster scenario, organizations may need to provide their employees and customers with alternatives to face-to-face meetings in the event of travel restrictions or social distancing policies. Additionally, organizations may need to disseminate critical business or operational information quickly and unambiguously to specific employees in real-time for effective disaster response coordination. Crisis management by global enterprises in times of regional, national, or global emergencies is critical to effective and consistent execution.

How we can help

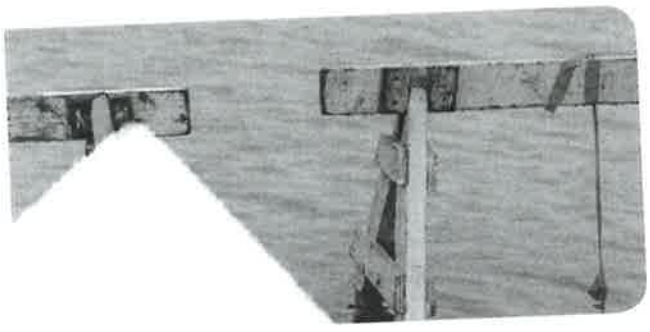
AT&T Unified Communications solutions provide real-time collaboration with others from any location, keeping the lines of communication open in an emergency. Businesses and government department/agencies can incorporate voice, Web, wireless and video into their emergency response communications processes.

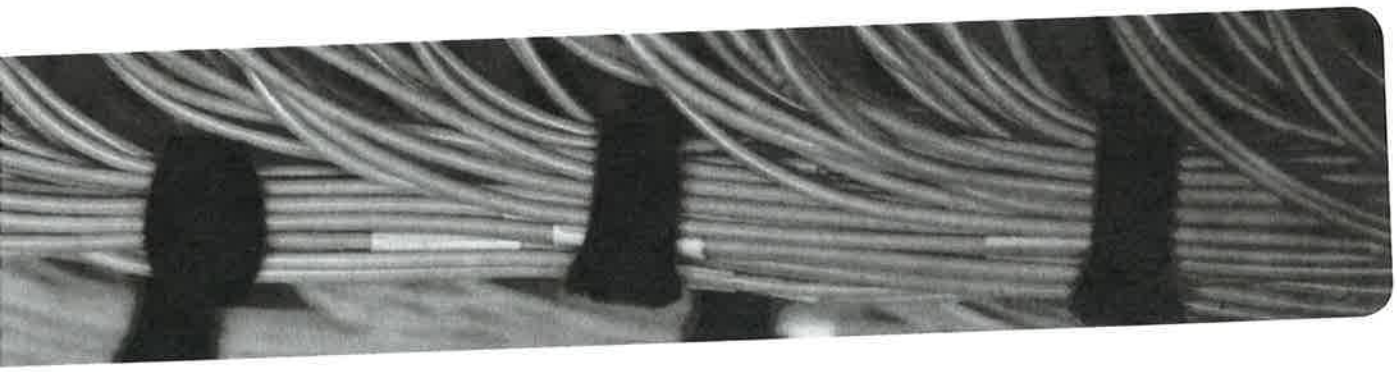
AT&T Conferencing with Cisco WebEx solution

AT&T Conferencing with Cisco WebEx solution offers real-time project collaboration for the critical operation of a business. Employees can communicate and collaborate real-time, viewing and editing documents and sharing applications to support the continuity of business operations. Key decision-makers and colleagues can collaborate on high-profile or emergency projects through an integrated global audio, Web and video conferencing solution, to help keep mission-critical business operations functioning. This HD video solution provides integrated conferencing and collaboration to help facilitate internal and external communication, from an array of devices, including mobile, laptop and multiple video endpoints.

AT&T Unified Communications Services (UC Services)

A cloud-based communication and collaboration solution that integrates multiple UC and telephony tools such as instant messaging (IM), voice calling, conferencing, and e-mail with presence, behind a single user interface – and makes them available via the AT&T network cloud. Businesses and government agencies are no stranger to disasters. With AT&T UC Services, even before arriving at the scene, emergency response personnel can make decisions about deploying equipment, securing the area and responding to almost any situation.





Emergency personnel can use the presence feature to verify who is available and send invitations to join an immediate Web conference utilizing instant messaging. Disaster relief teams can join the Web conference directly from IM, on mobile devices in the field or via desk phone while manning emergency operations centers. Each person can immediately view real-time status reports to plan and prepare recovery efforts. And since UC and telephony applications reside in the cloud, you gain the availability, redundancy and scalability of the AT&T network, helping you respond to disaster management more quickly.

Corporate crisis management service

For an added layer of security, AT&T offers firms the option of reserving ports on a separate network platform with priority access. This service is designed for critical executive level communications to reach key business decision-makers.

Web conferencing services

AT&T Conferencing with Cisco WebEx solution allows for real-time project collaboration critical to the operation of a business. The AT&T Web conferencing service adds a layer of communication effectiveness by allowing employees real-time viewing of business documents that support the ongoing continuity of business operations. In the event of an emergency, these same Web conferencing ports are designed to continue to function along with their associated audio conferencing ports and can be utilized for disaster-related collaboration. Key decision-makers can collaborate with an integrated audio, Web, video conferencing solution, on high-profile or emergency projects in order to keep mission-critical business operations functioning. And now you can join an AT&T Conferencing with Cisco WebEx solution using your iPhone® or iPad® from virtually anywhere in the world!

Collaboration – messaging

When planning for a pandemic event or any man-made or natural disaster, businesses need to consider their ability to maintain electronic communications, such as e-mail and voicemail. During any type of disaster, maintaining communications with employees, customers and shareholders is critical to managing through an event to keep everyone informed, mitigate panic and maintain critical business functions. In order to minimize the impact of an event, enterprises need to develop a plan to maintain their messaging infrastructure.

Business continuity/ disaster recovery challenge

In many types of disaster scenarios, businesses may need to relocate their local messaging infrastructure outside the impacted geographic area. If the messaging infrastructure is impacted, then personnel outside the affected area will need to assume the responsibility of monitoring and managing the messaging services. In addition, the security of the messaging service needs to remain intact.

How we can help

AT&T has a portfolio of messaging services to support a business during a disaster scenario. Key services include:

Hosted messaging

AT&T provides hosting and application management services for Microsoft Exchange in a highly available, global infrastructure. The AT&T server environment with state-of-the art security features, applies sophisticated backup systems to help prevent outages. Storage and networks are based on the AT&T utility computing platform, expanding and contracting as demand fluctuates. Hosted from data centers in the U.S., Europe, and Asia, the AT&T hosted e-mail solution brings 'enterprise-class' messaging and collaboration to customers in a scalable, redundant, and cost-effective way.

Secure Email Gateway

AT&T Secure Email Gateway (SEG) is a highly scalable, best in class email filtering and threat detection service, employing security tools such as encryption and predictive defense analytics to help keep your network safe from inside and outside threats. SEG is designed to block spam, viruses, and other inbound email threats before they reach your network and to filter outbound email to help protect your company against loss of important information. In the event of unexpected email downtime or disaster, the service also helps address your business continuity needs.

Enterprise paging

Enterprise paging is a text messaging gateway solution for group notification that works seamlessly with most business notification applications. Enterprise Paging uses the text messaging network, is backed by 24x7 technical support, and enables enhanced response features such as delivery confirmations, longer messages and rapid response prompts. Customers of Enterprise Paging can leverage the dial-up TAP protocol to add redundancy in the event of company e-mail server or Internet failures, and in the event of an on-premise outage the AT&T Business Notification Center Web site can be used as a backup to connect via the Internet from anywhere a connection can be established.

Remote access services/ mobility

Some studies estimate that if a pandemic becomes a reality, approximately 25-40% of employees may report to work from home due to illness or concerns with infection. For this reason several telework laws were enacted for federal, state and local governments to deploy effective strategies to support availability of personnel resources during an emergency. A Remote Access Plan becomes critical for supporting different types of employees and the applications to which they may need access. This is true for addressing any type of crisis, whether recovering from a natural disaster, such as a hurricane, or dealing with a man-made event such as a public-transit strike. A Remote Access Plan should be implemented in advance, at least in terms of the infrastructure, and include the ability to simply and easily deploy services to end-users on an as-needed basis. When natural disasters and unexpected events occur, it is absolutely vital that businesses respond quickly to maintain their customer service, minimize disruption to their business, and protect their business opportunities.

Business continuity/ disaster recovery challenge

When disaster strikes, a plan to provide remote access to critical applications is paramount to staying productive. Employees may scatter, whether moving to higher ground in the event of a hurricane or retreating to their home to avoid a pandemic. A Remote Access Plan should be developed and tested in advance to confirm that the different profiles of users have access to the equipment and software they need locally to access the corporate network remotely and scale their network in a timely manner to accommodate the spike in remote users. In addition, users remotely accessing corporate data from a variety of devices, smartphones and tablets introduce another layer of complexity and concern. The ability to manage mobile devices and provide corporate policies is key.

How we can help

AT&T provides a variety of access and VPN alternatives to meet the needs of multiple profiles. These services are designed to meet the remote access needs of users in both day-to-day business and in an emergency. Key services include:

Remote VPN access

AT&T offers a wide array of business continuity services designed to help facilitate your continuous operation including Remote Access to your VPN. This can extend the availability of your critical business processes, applications, data, work centers and networks for your employees. AT&T Network-based IP Remote Access extends your network virtually anywhere Internet connectivity exists and provides near seamless integration of applications and helps scale your remote access infrastructure to accommodate the increase in remote users. In addition, AT&T Network-based IP Remote Access integrates mobile technologies and services as an extension to existing enterprise infrastructure.

AT&T also offers SSL (Secure Socket Layer) encryption, allowing end-users access to specific applications via a browser from any location via virtually any device (e.g., Smartphone, PC, laptop, tablet) wherever Internet access is available.

AT&T remote access VPN services also supports SSL and is most appropriate for end-users who don't have access to a company-provided machine and/or only require access to a few Web-enabled applications such as e-mail.

Access virtually any time, any place

AT&T provides a range of access methods, including Wi-Fi, Wired Ethernet, Wireless, Wireless WAN, ISDN, DSL and Dial-Up. The AT&T Global Network customer takes the guesswork out of which access method is available by automatically detecting available access methods and connecting in priority order to the first available method. In addition, network congestion is minimized by proactive monitoring of the AT&T network and augmenting capacity as required.

Wireless WAN Connectivity

As part of a disaster preparedness program, AT&T can provide the ability for enterprises to connect to network resources when wireline solutions are not available or are being restored, reducing the costs associated with downtime. WWAN Connectivity from AT&T provides diverse, cost-effective backup for data applications, quick deployment for remote locations, temporary locations for mobile workers and consistent network connectivity. WWAN offers a truly diverse backup solution for mission-critical data when a landline outage occurs. Plus, with a WWAN solution, businesses can utilize their existing security infrastructure and choose from a number of additional security options for network-to-network connectivity.

Mobile Remote Access

Mobile Remote Access Services support end-to-end connectivity for corporate networks from any location, using a multitude of devices. It gives all users flexible, highly secure access to corporate assets, thereby empowering a genuinely mobile workforce.

The AT&T wireless network provides the coverage, performance, security and convenience enterprise customers need. We can support multiple current and most popular platforms, with options for laptops, embedded devices, integrated devices, smartphones, tablets and the use of mobile hot spots. The AT&T Global Network customer provides a simple user interface, with one-click network access and integrated VPN support. And AT&T VPN solutions offer a wide variety of service levels and network configurations, all supported by our global MPLS-enabled network.

Customers can quickly configure and deploy their devices where and when they need them in areas where there is wireless, Wi-Fi or dial-up access so that users can connect while they are on-the-go or if displaced in the event of a disaster.

Wireless Push-To-Talk

AT&T Enhanced Push-to-Talk customers value the convenience and productivity of being able to set up individual or group calls with the push of a button and instantly communicate a message over the speaker of the recipient's handset. This saves them time as they no longer have to dial, answer and go through greetings, etc., before communicating. For example, in an emergency, a dispatcher can communicate location and instructions over Push-to-Talk faster than it would take most emergency responders to answer a ringing phone. For repair crew, receiving messages on their handset without having to hold a phone and make a connection is more convenient and allows them to continue working while talking.

Enterprise Mobile Management (EMM)

When developing a disaster preparedness plan, consideration must be given to users and the disparate devices and operating systems they are using to access the organization's infrastructure, as well as the sensitivity of the corporate data being accessed. AT&T provides enterprise mobile device management and security solutions that empower IT managers to set policies, lockdown applications, expand on-device encryption, distribute software, conduct device diagnostics, understand inventory, and more. These comprehensive, scalable device management and security solutions provide IT managers with the capabilities to help protect corporate data on a day-to-day operational basis, as well as in an emergency. AT&T also offers professional services options to assist IT managers with developing a holistic mobile strategy - from consulting, design and development, to deployment and support.

AT&T Private Mobile Connection

AT&T provides reliable standards-based connectivity between enterprise data center locations and its wireless network. It is through connections that data traffic from wireless devices can be aggregated into one or more AT&T locations and transported to customer data centers. Geo-redundancy within the wireless network from AT&T allows traffic to be shifted to unaffected locations during disaster scenarios. By using this product as part of a business continuity solution, a customer's network and security infrastructure can be economically utilized to help support continued service during times of emergency. AT&T Private Mobile Connection enables the seamless use of wireless applications during disaster recovery scenarios, providing the security features and reliability elements that enterprises require regardless of transport medium.

Crisis phone program/voluntary suspend

As an integral part of disaster preparedness planning, AT&T offers customers a Crisis Phone Program to facilitate remote access and mobility. This program provides devices for organizations to use solely in emergencies. Enterprise customers can manage costs by keeping devices on-hand in a "voluntary suspend" mode, ready to be activated only when a crisis or emergency arises.

Contact center

When natural disasters and unexpected events occur, it is absolutely vital to minimize risk to employees, operations and protect essential assets. With a contact center serving as the front door to the business, maintaining a fully functional contact center can be the lifeline for how enterprises manage through crisis events.

Business continuity/ disaster recovery challenge

Businesses need to be protected against all of the vulnerabilities to a contact center that arise when disaster strikes. Networking infrastructure needs to be highly resilient. Call routing needs to be flexible and adaptive in the event of limited resources. Call completion needs to be streamlined and highly automated to minimize agent involvement when people are impacted.

How we can help

AT&T Contact Center Services are ideally suited to help businesses respond quickly to unexpected events. Through an array of advanced capabilities, AT&T Contact Center Services work to support continued customer operations. With highly-skilled Consulting and Integration Solutions resources, AT&T works with businesses throughout the Contact Center life cycle, from pre-planning all the way to day-to-day operations for end-to-end optimization to enable continued and non-disrupted business activities. Our networking services are highly-scalable and resilient. The AT&T portfolio of call routing solutions allows calls to be automatically delivered to the appropriate destination. With an array of automation services, call fulfillment can be accomplished in a highly efficient and effective manner. AT&T uses a "predictive, preventive and proactive" approach through its network service offerings. Based on predicting problems in advance and building intelligent systems and alarms into the network, AT&T initiates rules and procedures to provide network availability for uninterrupted service. AT&T has a number of product and service offerings that specifically address the challenges of business continuity including offers hosted in the AT&T network or premises-based at the customer site and options for fully dedicated or shared environments. Within the toll-free network, AT&T provides a number of solutions that give customers a high degree of flexibility and control when using either traditional delivery methods or IP. Solutions offered within the AT&T toll-free network include:

AT&T Route It!℠
Provides organizations with the ability to manage toll-free calls virtually any way they need. As the need to respond to emergency situations arise, businesses can develop new routing plans and invoke alternate business rules to direct calls to the most available resources at the time.

Alternate destination routing
Provides predefined network routing schemes that automatically redirect calls when a busy or ring-no-answer condition is encountered.

Next available agent routing and network queuing
The combination of these two capabilities provides businesses the ability to queue calls in the AT&T network and route to the customer location when agents become available. This feature extends and enhances the traditional premises-based capabilities and allows callers to wait for an available resource when active agents are unavailable.

SIP routing
Utilizing network-based Session Initiation Protocol (SIP) routing capabilities of our IP toll-free offering provides the ability to get customers to the right customer service centers that are available to address their needs the first time.

AT&T Contact Center Services
Provide a variety of hosted and managed service offerings that enable continued business operations during disruptive situations. These offerings include hosted and managed services that provide voice enabled self-service applications, automated routing, and multi-channel customer contact functionality. Our Contact Center Services also provide quick and immediate response to adverse and unexpected conditions while maintaining customer service. The dynamic distribution of call flows reduces the risk of single-point-of-failure within the call center environment. Businesses can face uncertainty with confidence knowing that their customer-facing operations are backed by world-class network reliability and resiliency.

Hosting & application management

When planning for any type of disaster, public and private sector establishments need to consider a geographically diverse strategy for maintaining availability and access to mission-critical applications. During an event, hardware, software, processes and personnel can be adversely impacted. In order to mitigate this risk, customers need to develop a plan to quickly re-establish their application infrastructure and recover data.

Business continuity/ disaster recovery challenge

In a disaster scenario, such as an earthquake or terrorist attack, businesses may need to temporarily fail-over applications and infrastructure to another geography. In the event of a pandemic, local personnel responsible for the applications and infrastructure could be impacted. Firms need to have the ability to turn up application instances and infrastructure, rapidly recover data and vital records, and maintain the availability of their mission-critical applications.

How we can help

AT&T offers an unparalleled breadth of application management and hosting services, as well as associated consulting services, to support application availability and high availability access to critical data and applications. AT&T also offers a complete range of storage services to meet recovery time and recovery point objectives. However, for the purposes of planning for Business Continuity/Disaster Recovery, there are a few services that should be strongly considered:

Hosting services

AT&T provides flexible hosting solutions so critical business data and applications remain accessible and high-performing. AT&T has the ability to design, implement, monitor, manage and report on the availability and performance of infrastructure, servers and applications. With diverse capabilities such as collocation, managed hosting, utility computing, and Web hosting, AT&T meets the diverse needs of organizations that need to create a comprehensive recovery strategy. In addition, AT&T provides highly-reliable conditioned space that has direct access to the AT&T Global IP Network for immediate access to your infrastructure and applications.

Cloud services

AT&T Cloud Services provide a flexible, cost-effective alternative for delivering IT services – in a way that complements existing systems, staff and processes. Procurement and deployment normally takes time and ties up internal staff. With self-service provisioning, AT&T cloud solutions let organizations sign up online and tap into virtual AT&T infrastructures within minutes. You can launch new services, applications and projects rapidly and expand access, capacity and performance on-demand, while you view and monitor consumption via a Web-based portal.

Application management

AT&T manages and provides ongoing support for the key software applications companies rely on, specializing in managed enterprise software solutions, eCommerce, and messaging applications. AT&T hosts and manages mission-critical applications, including maintaining replication and disaster recovery for the applications that help businesses operate. AT&T proactively monitors, maintains, provides help desk support, patches, fixes and updates applications – so that in the event of a disaster, customers can concentrate on their core business rather than getting their applications up and running.

Managed data storage services

AT&T provides primary storage through its Ultravailable™ Storage and Storage Plus services for customers who either co-locate or host their IT infrastructure within an AT&T Internet Data Center (IDC). AT&T also offers backup and recovery data storage services through its tape and disk backup and restore capabilities which provides businesses with

a highly secure and recoverable environment for their data. A Web interface provides the ability to manage and restore data, as needed. Backup copies can be directed to a specified location or an AT&T Internet Data Center.

Data mirroring/replication

For synchronous mirroring/replication requirements, customers may elect to use AT&T Ultravailable™ Network as a high-end, highly-available, fault tolerant, fully redundant, optical networking solution.

Content distribution

AT&T Content Delivery Network service replicates and distributes your Web page content, files for download, and live and on-demand video, allowing you to efficiently distribute your content to your customers and significantly improve your Web site's capacity, reliability and performance. So even if your Web server or data center fails, you can count on AT&T to continue to distribute your content hosted in our network of streaming and caching EDGE servers.

Digital signage

AT&T Digital Signage™ service is a managed solution that delivers your multimedia message content, interactive wireless Apps, and content creation services. The Service is very flexible in scalability as it leverages your firm's internal unicast or multicast distribution network or Internet connectivity. AT&T Digital Signage™ service includes full life cycle support for design, global deployment, monitoring, maintenance, and break-fix. AT&T even provides support to create the content that will be played on the signs and how to leverage marketing techniques for customer interaction.

Consulting services (AT&T consulting)

As part of their Cloud and Data Center Transformation practice, AT&T Consulting provides a broad portfolio of Business Continuity/Disaster Recovery (BC/DR) services to our customers:

- BC/DR Strategy and Roadmap Engagements
- BC/DR Infrastructure Assessments
- BC/DR Application Assessments
- BC/DR Facility Assessments
- BC/DR Design and Integration Services

AT&T Consulting possesses a team of industry-leading, certified and experienced business continuity experts to facilitate the creation of a Risk Assessment (RA), Business Impact Analysis (BIA) and a Business Continuity Plan (BCP), which also addresses the necessary Disaster Recovery Plan (DRP) for our customer's environment. The DRP provides the necessary Runbooks and Continuity of Operations Processes (COOPs) which are required to successfully execute the DRP and recover mission-critical voice and data services. The COOPs also address the processes you may execute in response to the loss of a critical facility as well as situations where access to the critical facility is blocked or hampered by the disaster event.

One factor that is frequently overlooked in the design and implementation of DR solutions is the integration of the DR environment into the production environment from an operational perspective. These environments must be instrumented and monitored as if they are part of the production environment. As part of our methodology, AT&T Consulting addresses how the DR solution will be integrated into the production environment and also helps ensure that the DR environment is capable of being managed and monitored on the DR site as well as remotely at a Global Operations Center.

The AT&T Consulting team has the flexibility to either create BCPs where none currently exist or to evaluate and modify existing BCPs. They will also confirm that critical enterprise business processes have documented BCPs that are updated and tested on a regular basis. Table Top Plan exercises are designed around specific scenarios to test the viability and capability of the plans, as well as to train key executives on their responsibilities during a disaster. The maintenance of the BCP and regular Table Top test execution are focused on the concept of continuous improvement of the BCP with the objective of achieving continuous business operations.

AT&T enterprise recovery services

Maintaining a business continuity and recovery program requires expertise and resources that may not be readily available in-house. Enterprise Recovery Services from AT&T offer a full portfolio of subscription-based disaster recovery services for systems and user work locations for businesses to remain prepared for any unplanned event that impacts their company's operations.

Business continuity/ disaster recovery challenge

A business depends on constant, uninterrupted access to key applications and critical data. To mitigate the repercussions of a disaster, business continuity and recovery planning is essential to support continued access to business processes. Not only is it important to understand what to recover, whether it is information systems or work group space for employees that have been displaced by a disaster, it is also necessary to know where information systems will be reconstituted or end-users supported.

How we can help

AT&T offers a choice for recovery utilizing center-based, mobile-based or subscriber location-based recovery options for information systems and employees, telecommunications capabilities and IT resources. Key services include:

Systems recovery

AT&T ERS System Recovery solution is ideal for organizations that need to recover distributed systems, Intel®-based platforms, and/or mainframe systems. The solution supports over 30 current and legacy platforms, as well as sophisticated storage environments, and the network to keep it all connected.

End-user recovery

AT&T End-User Recovery Service is ideal for organizations that need alternate workspace for their employees, telecommunications capabilities and IT resources to recover their business processes. End-User Recovery resources includes space, equipment and voice and data communication lines. ERS solution delivery options:

- Center-based recovery solution
  This solution offers office space and conditioned IT facilities strategically located throughout North America where the affected employees or COOP personnel can quickly resume business operations in the event of loss or disruption of their location.

- Mobile-based recovery solution
  The mobile recovery center solution is designed to save businesses time and to keep their employees closer to home. During a disaster, personnel can focus on assessing the extent of damage caused by the disaster and implementing the contingency plan, while the AT&T-provided Mobile Recovery Center is en route to their specified location. Mobile Recovery Centers are equipped with office space, communications and open systems. The mobile recovery center can be configured with generator power as well as satellite communications.

- ERS quick ship
  This solution will quick ship pre-specified equipment to the customer specified site at time of disaster.

Managing network security

When planning for any catastrophic event, security should be at the top of the list of services to review. Recovery time and data integrity are paramount to business operations. In order to minimize the impact of an event, alternatives to local or premises-based solutions should be evaluated.

Business continuity/ disaster recovery challenge

During a natural or man-made event, businesses may have new temporary locations and significantly increased numbers of employees accessing their network from remote locations. More than ever, businesses will be faced with the need for better secured access to their corporate WANs and LANs. In addition, local security infrastructure and trained personnel could be impacted by the event. Businesses need to have the ability to monitor and manage the security infrastructure during the event.

How we can help

With extensive security experience, and a variety of security resources, AT&T is well equipped to help protect a firm's WAN, LAN and Remote Access services. For the purposes of Business Continuity/Disaster Recovery planning, there are a few capabilities that firms should strongly consider. Key services include:

Firewall protection

The experts at AT&T can help design and implement premises-based and network-based firewalls that will help detect and filter out malicious traffic in the network before it gets to a customer's premises. AT&T can also provide a network-based firewall solution that allows remote workers as well as LAN users to access corporate applications in a highly secure manner. In addition, AT&T offers an Endpoint Security service that is located on the users' desktops or notebooks and provides a means of maintaining the customer's corporate security policy by helping to protect the endpoint as well as the corporate network from various threats and malware. The goal of AT&T is to help organizations maintain their network security during an event.

Intrusion detection/prevention

AT&T Managed Intrusion Detection/Prevention Service helps protect the networking infrastructure by detecting and responding to unauthorized attempts to access the customer's network. The hardware/software application is connected to the AT&T Security Operations Center where service technicians support round-the-clock surveillance. When a pattern of misuse is detected, the system quickly and automatically responds according to predefined policies to send an alert and take immediate action.

DDoS Defense

AT&T Distributed Denial of Service (DDoS) Defense helps detect and mitigate DDoS attacks. DDoS identification and mitigation takes place within the AT&T IP backbone providing increased DDoS protection from malicious traffic before it reaches the customer's network. If a volumetric denial of service attack is detected, the traffic will be routed to a network mitigation scrubbing facility, where the malicious DDoS attack packets are identified and dropped while the traffic determined to be valid is allowed to pass to the customer.

Bundled firewall, email and web security

AT&T Secure Network Gateway (SNG) is a cloud-based security service that includes AT&T Network-based Firewall Service, AT&T Secure Email Gateway Service and AT&T Web Security Service. With Secure Network Gateway, customers have tools to help them protect their e-mail from viruses, worms, and spam; manage Internet access with firewalls; block Web-born malware from corporate networks; and receive alerts about possible attacks.

Mobile security

AT&T Mobile Security network-based features help maintain compliance with government regulations, enforce corporate security policies, and simplify the management of personal or enterprise-owned devices. AT&T Mobile Security provides anti-virus, anti-malware, and anti-spam capabilities, loss and theft protection, and application monitoring and control. Device management features that quickly and easily protect, manage, and locate lost mobile devices are also included. These solutions also provide consistent application of your corporate security policy when your wireless device connects back to your network. You can validate that your wireline and wireless devices adhere to the same security policies. AT&T provides a range of MDM solutions and professional services that empower IT managers to set policies, lockdown applications, expand on-device encryption, distribute software, conduct device diagnostics, understand inventory, and more. These comprehensive, scalable device management and security solutions provide IT managers with the capabilities to help protect corporate data on a day-to-day operational basis, as well as in an emergency.

AT&T Threat Manager – Log Analysis (TMLA)

AT&T Threat Manager – Log Analysis (TMLA) delivers near real-time log monitoring, correlation and expert analysis of security activity across your organization. This service helps to improve the effectiveness of customer's security infrastructure by actively analyzing logs and alerts from the customer devices in near real time, 24x7. Our experts provide prioritization and notification around high and critical severity security incidents.

At the core of this solution is AT&T Threat Intellect: The culmination of eight global security operations centers, our advanced data analytics and the rapid results of machine learning. One of the benefits this overarching solution brings to your organization is reduced noise of traffic at volume, helping to improve your security infrastructure by actively analyzing logs and alerts from your devices in near real time, 24x7x365.

AT&T Threat Manager – Log Analysis provides a broad view of the security in your network by helping to efficiently correlate alerts from multiple devices and device types across the entire enterprise:

- Utilizes AT&T proprietary data and insights, and 3rd party feeds
- Distills billions of raw logs to a few cases
- Helps detect threats earlier
- Implementation support can be added and provided by AT&T consulting for asset identification and implementation verification

More information on all of these business solutions can be found at the following URLs:

att.com/security

wireless.att.com/businesscenter

AT&T customer support

Communications

During a disaster scenario, AT&T communicates with its customers through a variety of vehicles including, AT&T BusinessDirect® | AT&T Premier, AT&T Vital Connections, broadcast e-mails, individual e-mails or phone calls from AT&T representatives, and Interactive Voice Responses. Methods of communication vary based on the severity and proliferation of an event. AT&T communicates internally when an event occurs and then communicates with its customers as appropriate information becomes available.

In addition, customers can obtain updates directly from AT&T in a self-service fashion using att.com as the front door to any updates regarding events. As a standard feature on att.com, there is information about business continuity, both about how AT&T is prepared and ready through its NDR exercises, and about services that are available to customers for their preparedness requirements.

AT&T BusinessDirect® | AT&T Premier

AT&T BusinessDirect® | AT&T Premier is a suite of powerful online tools that can be particularly helpful for both communications and self-servicing for AT&T customers during times of disaster. These tools can be used to reroute network traffic, test circuits, report and track service problems, place emergency orders, and perform other customer service related tasks. It is important to be prepared to be able to use the tools when they are needed. Therefore, customers should confirm they have access to and are familiar with the portal before an unexpected incident occurs. Customers can obtain access to the portal through their AT&T account representatives.

During a disaster, AT&T will post critical information and messages for customers on the AT&T BusinessDirect® | AT&T Premier for easy access. There are several ways in which businesses can use AT&T BusinessDirect® | AT&T Premier, as depicted in the following table.

AT&T BusinessDirect® | AT&T Premier online tools may be used within business continuity planning and recovery efforts.

AT&T BusinessDirect® | AT&T Premier online tools may be used within business continuity planning and recovery efforts

AT&T BusinessDirect® capabilities	Tool name	Applicable service(s)
Call routing • Make changes to existing routing plans in near real-time. Shift toll-free traffic to other contact centers to maintain customer service • Establish new routing plans. Add new terminations in near real-time and begin routing terminations almost immediately	• Control Toll-Free Routing • Route It![s]	• AT&T Toll-Free Service
eMaintenance • Check networks for outages in near real-time • Test circuits to see if they are performing properly • Submit trouble tickets to initiate repairs quickly • Invoke Service Assurance Plans – toll-free call routing plans that are prepared in advance	• AT&T BusinessDirect Map • AT&T BusinessDirect eMaintenance	• Most Domestic and International Data Services • Outbound Switched Voice Service (EM only) • Domestic and International Toll-Free Readyline Service • Dedicated Voice Service • Domestic and International Toll-Free MEGACOM Service • Most AT&T Managed Services
eOrdering • Move, add, change and disconnect services on AT&T network • Receive up-to-date network inventory • Get near real-time status on orders	• AT&T BusinessDirect eOrder • AT&T BusinessDirect Map	• Most Domestic Voice and Data Services • AT&T Toll-Free Service • IP-Enabled Frame Relay and ATM Services
Performance reporting and monitoring • Originating and terminating details on calls reaching the customer's premises • Summary information on call attempts to the customer's toll-free number • Near real-time information on AT&T High-Speed Packet Service ports and PVC usage • Monitor data circuits: for T1 circuits, configuration, performance and fault monitoring; for T3 circuits, configuration and fault monitoring • Near real-time fault notification on trunk and carrier outages • Site availability for routers; site-to-site latency by Class of Service; near real-time usage for site latency and packet delivery by COS	• Analyze and Monitor Call Data • Analyze Toll-Free Call Attempts – Real-Time • AT&T BusinessDirect Map • Customer Network Management Service/Web Reports Interface • iGEMS T1-T3 Monitor • IP Network Usage Reports Monitor and Control Voice Performance	• Frame Relay Service • ATM Service • Private Line Service • IP-Enabled Frame Relay and ATM Services • Domestic and International Toll-Free Voice Service • Dedicated inbound and outbound domestic long distance voice trunk groups • AT&T Enhanced VPN Service • AT&T Advanced VPN Service

How online tools to manage your wireless environment may be used within business continuity planning and recovery efforts

Premier enterprise portal	Tool name	Applicable service(s)
• Purchase, move, add and change wireless services, features and devices during and after a disaster based on customer's contract and device preferences • End-user self service for online wireless account management, bill payment and care any time	• Premier Resource Center, Premier Online Care • Individual, Corporate and Telecom Manager Online Stores	• Most Enterprise Wireless Voice and Data Programs and Services
Online activation, SIM inventory management and simplified billing • Order inactive data Subscriber Identity Module (SIM) cards online before disaster strikes • Online activation of the SIMs needed during an emergency • Online Billing – view a simplified bill • Online ticket entry, status and reporting	• Enterprise On-Demand Service	For large wireless data deployments such as: • Field Service; ruggedized devices • Telemetry; meter reading devices • Dedicated Voice Service • Point of Sale; merchant devices • Mobile Professionals; LaptopConnect cards
Service coverage maps • Provides interactive wireless network coverage map detail for wireless voice, data and partner networks • Zoom to the street level to help establish service expectations if company resources are displaced	• Coverage Viewer	• AT&T-owned GSM, GPRS and EDGE wireless network service • 3G/4G HSPA+/4G LTE wireless network • Unaffiliated carriers, partner coverage

Wireless service not available in all areas. Due to transmission, system and other limitations, wireless service may not be accessible at all times. Offer(s) subject to change. Additional restrictions apply. See https://www.wireless.att.com/businesscenter/solutions/ for more information.

Additional information

It's important to identify accurate sources of information for preparedness efforts. The AT&T Web site, Vital Connections, provides disaster and business continuity resources providing guidance and assistance in addressing your needs. Additional information on Business Continuity planning can also be found on AT&T Networking Exchange, the following government and agency Web sites and by contacting your AT&T Representative.

AT&T sites:

- AT&T Vital Connections
  att.com/vitalconnections
- AT&T Networking Exchange
  att.com/networkingexchange/businesscontinuity
- AT&T Doing Business with us
  att.com/dbw

Non-AT&T sites:

- BCI Standards and Guidelines
  thebci.org
- Federal Emergency Management Agency (FEMA) - Ready
  ready.gov
- Federal Emergency Management Agency (FEMA)
  fema.gov
- Federal Emergency Management Agency (FEMA) PS-Prep
  fema.gov/privatesector/preparedness
- National Security Telecommunications Advisory Committee (NSTAC)
  dhs.gov/nstac
- NCS - TSP Program Office
  tsp.ncs.gov
- NOAA North Atlantic Hurricane Outlook
  noaa.gov
- U.S. Health and Human Services
  pandemicflu.gov
- World Health Organization
  who.int
- Centers for Disease Control and Prevention (CDC)
  cdc.gov

06/20/16 AB-0771-09
©2016 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

Attachment One – Technical Requirements Matrix

Bidder Name: Rave Mobile Safety

Each of the items in the Detailed Requirement Matrix in the table below requires a response of one of the following options: "Yes", "3rd Party", "Next Release", and "No". Bidders must respond to the Detailed Requirements Matrix using the matrix format provided and must not reorder the requirements.

The bidder's response must provide enough detail in narrative form to allow the Evaluation Committee to score the bidder's approach to each technical specification.

Only one box may be checked per requirement. If software demonstrations are requested, you may be asked to demonstrate each item marked as "Yes".

The Bidder Response box should be completed if the response to the requirement is "Yes", "3rd Party", or "Next Release". Bidders may also use it with No response if desired. Bidders must provide a response directly in the matrix, using as much space as needed. Explain each response and describe how the proposed solution meets each requirement. Responses do not need to be limited to one line.

Below is a brief definition of each response option. Bidders should carefully read the response definitions as these responses, as well as the entire response to this RFP, will become part of any resulting contract with the awarded contractor.

Yes	Yes, requirement is met and demonstrable in the current release of the product(s) proposed in the bidder's response to this RFP, without manipulation of fields, forms, or the need to add fields or tables to the system.
3rd Party	This requirement is met through the use of a 3rd Party Vendor's product, which is included as part of this proposal. Costs associated with 3rd Party products used to satisfy any requirement must be included in the fixed price cost of the proposed solution.
Next Release	This option should only be used if the requirement will be part of the next release of the product(s) included in the proposed solution. To meet the criteria for using this response, the "next release" must already have an established release date and a published list of what will be included in this release that includes the specific requirement. Established release date must not exceed 6 months from date of proposal.
No	No, the requirement is not or cannot be met by the product(s) included in the proposed solution. A response of "No" to a requirement does not eliminate the bidder's proposal from consideration. All proposals meeting the mandatory requirements set forth in Section II.N will be evaluated and scored by the evaluation committee.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

	The "No" option is also appropriate when a requirement can be met through a separate module or if the module is not included in the fixed price cost proposal. In the above scenario, it is recommended that the bidder note this in the "clarification" section for the requirement and include pricing, if available in Appendix A – section - Optional Products and Services.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

	General Service Requirements Section 1	Yes	3rd Party	Next Release	No
1.1	The emergency mass notification services (EMNS) must be able to reliably and efficiently distribute and manage message notifications through any and all of the following multiple channels. a. Telephony calls to landline/wired phone, including Voice over IP (VoIP); b. Wireless mobile devices; c. SMS, text to wireless mobile devices; d. Mobile device apps; e. Email; f. Desktops; g. Social media such as Facebook and Twitter; h. Common Alerting Protocol (CAP feed), and; i. TTY for hearing impaired. If bidder supports additional channels not listed above, please list them in the space provided below. Describe how the solution will meet this requirement.	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Business

Figure 1: Rave Alert uses a single activation to send messages by all available selected delivery modes.

Telephony calls to landline/wired phone, including Voice over IP (VoIP);

Compliant. Rave's voice services use a combination of VoIP and TDM/SS7 on a variety of high-quality carriers including AT&T, XO, Verizon, Sprint, Level 3, ANI, and Impact. We draw on a capacity pool of over 40,000 calls per minute from 4 geographically redundant calling centers and our delivery systems use real-time congestion management to avoid overwhelming local exchanges. Rave's voice systems automatically detect and appropriately address TTY/TDD devices used by people with disabilities. We support voice alerts as well as SMS messaging on over 200 international carrier networks, so you can reach your recipients wherever they are.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Wireless mobile devices;

Compliant.

SMS, text to wireless mobile devices;

Compliant. Rave Mobile Safety uses a combination of methods to maximize delivery success rates across the broadest spectrum of carriers. Rave Alert works for four of the five top-tier SMPP message aggregators in the US, supporting high volume connectivity providing both strong performance and redundancy and message failover when networks experience faults outside of Rave's controls. Rave also maintains direct high-volume binds to AT&T Wireless, Sprint, and T-Mobile, as well as to specific regional carriers with a substantial presence in our customer base. These binds are redundant with our connections to multiple Tier 1 SMPP aggregators and other networks.

Mode of Delivery	Max Rate of contacts	Throughput Tiers	Typical Production Rate	Key Bottlenecks
SMS (SMPP)	2,700+ messages/sec	10 min = 1.62M 30 min = 4.86M 60 min = 9.72M 120 min = 19.44M	600 - 1000+ messages/sec	Cell site capacity

Carrier Coverage

To make sure you reach your SMS subscribers, Rave Mobile Safety currently supports ***all* US-based carriers** and **over 200 international carriers.** Rave Alert supports 2-way SMS communications using SMPP protocol by default. A few lower-tier carriers do not yet support SMPP protocol. In these cases, Rave automatically uses the carrier's supported SMTP protocol. Clients never have to specify which protocol to use; the optimal delivery path is managed by Rave Alert.

We validate all incoming SMS phone numbers with automated carrier lookups and detection of active status on US carrier networks. When recipients add mobile numbers through our user portal, a 2-step validation ensures they are really in possession

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

of the device they entered, and are not simply entering a valid mobile number belonging to someone else. Rave Alert also periodically re-validates whether each number is still active on the initial carrier. The system automatically captures potential issues in standard reporting.

When a number changes carriers, our automatic re-validation detects and records this change within a 72-hour window, revalidates the number, and applies changes as appropriate.

Redundant SMS Delivery Networks

The majority of U.S. SMS messages are delivered through SMS aggregators, firms that route traffic between content providers and Tier 1 mobile carriers and aggregator networks using a sophisticated number and carrier lookup database.

Unfortunately, SMS aggregator routing infrastructure is immature and suffers from reliability issues at times. This poses challenges for emergency notification vendors like us working to maintain the highest degree of resilience both within and outside our hosted infrastructure.

Rave Mobile Safety maintains relationships with multiple premium SMS aggregators and very high contracted capacities so that we can still deliver messages even when an aggregator has an outage. When an individual number isn't reached with the first message, Rave Alert has automated retries to intelligently try again. Rave Mobile Safety is the only vendor in our space that provides redundancy both across aggregators and within each individual aggregator. For each aggregator, we maintain multiple live, concurrent, simultaneous high volume binds on separate servers.

Our long experience with aggregators and related outages also helps improve our delivery. Rave Mobile Safety has managed high volume SMS delivery for well over a decade. Our system has weathered events where the infrastructure was distressed such as the Boston Marathon bombings, Great Shakeout mass messaging tests in all US time zones, and numerous "superstorm" systems. We invest in our infrastructure directly in response to these real-world stress-tests, building redundancy as a remedy to aggregator and carrier faults.

Our many delivery paths, from redundant aggregator to carrier connections, achieve industry-leading delivery performance. And on average days, when all delivery paths are fully available, Rave Alert automatically balances system load across all of them to achieve our industry-leading performance.

Support for Second and Third Tier Carriers

While the top 4 carriers serve most U.S. mobile customers, a long list of Tier 2 and Tier 3 tier carriers have strong presence in

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

particular cities or regions or among certain demographic groups. These types of carriers include many pre-paid plan providers and resellers of services licensed from the major carrier networks (often referred to as "MVNOs"). Rave Alert supports messaging to all US-based carriers, so you can reach your recipients no matter what small carrier they use.

More, the carrier landscape changes regularly. We maintain mature and ongoing service processes to follow these changes and automatically incorporate them into our product reach. We continuously update our carrier support through industry consolidation, changes in licensing policy, support for network changes, and more. You can count on us to continue managing delivery to the widest possible range of carriers as these changes continue.

We incorporate carrier management directly into our support protocols, allowing us to thoroughly address changes in the carrier landscape both at the service level and when reported by individual recipients. We work hard to make carrier management seamless for our customers. When that's not possible, such as when carrier outages have delivery impacts, we will announce these conditions on the administrator console as long as they are relevant.

Mobile device apps;

Compliant. Anyone with the mobile app from any jurisdiction can receive a push notification of a geo-targeted public notification. This means that visitors to any area will be notified of a serious message. Also, the user is able to browse a map view and highlight active alerts and see their content. Messages collect in an Inbox view, and each message can be viewed and if desired spoken to the user.

Our public recipient mobile app contains features that display a map view based on a user's current location but which can also be browsed. Any public notification designated to use the app as a delivery mode will be showing a map pin view where the user may view and review current alerts. In addition, app users from anywhere in the US will see 2 delivery behaviors:

1. If they are found within view of a geo-targeted notification, they will receive a push notification of your message.
2. When a geographic selection is NOT applied to an outbound alert, the user would see only the map PIN and not the message unless they are specifically opted-in to the jurisdiction or are found within the jurisdictional boundary.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

In addition, all household addresses entered in the app or on the public portal with affiliated Rave Alert jurisdictions will see opt-in choices for each jurisdiction with an address in the user's profile. Similarly, when automated reminders send the user back to either portal, the user will be shown any new offerings falling within their address-based locations.

Email;

Compliant. Rave Alert has the capacity to send 60,000 emails per minute, or over 3 million emails per hour.

None of our clients have the local infrastructure to support such high throughputs. We maintain these high capacities so we can always output the highest number of calls your infrastructure can tolerate. Delivery speed depends on how many emails local infrastructure like email server capacities can support. On average our clients receive between 54,000 and 3.6 million emails delivered per hour.

These delivery speeds vary so much because of variations in email systems, but also because Rave Alert offers tools so you can fine-tune message output to your SMTP server capacity, optimizing delivery rates. Working with customers, Rave has been able to exceed customer expectations on email delivery to internal email servers. Rave performance with large public network providers such as Google, Microsoft, Yahoo! and others, is typically very strong, given the excellent capacities supported by those networks. Rave maintains agreements with key public network providers to facilitate optimal delivery rates.

The table below describes typical email metrics:

Mode of Delivery	Max Rate of contacts	Throughput Tiers	Typical Production Rate	Key Bottlenecks
Email	1,000+ messages/sec	10 min = 600,000 30 min = 1,8M 60 min = 3.6M 120 min = 7.2M	15-1000 messages/sec (highly dependent on configuration options as well as capacity of client email servers)	Recipient's email server capacity; connections may be tuned to capacity

Desktops;

Compliant. Rave Alert integrates with many third-party solutions providers, often via RSS, CAP, or some other direct integration method. Please note that unlike nearly all other requirements for notifications, desktop notification nearly always requires the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

configuration of some on-premise or on-network resources that manage notification initiations as well as configure each supported desktop chosen.

Please note that pricing worksheets provided with this bid do not provide specific pricing on these options; a premise-based desktop notification option is not included with this bid response. If required, Rave Mobile Safety can provide additional information upon request.

Social media such as Facebook and Twitter;

Compliant. You can post directly to Twitter and Facebook. You can post to specific Twitter pages, Facebook wall feeds, or groups, and limit alert author access to specific sites and accounts as needed. We support unlimited Twitter accounts and Facebook pages, wall feeds and group structures.

We offer role-based access controls that enable different administrators to post to different social media pages, so your participating organizations can update their own pages and feeds.

Common Alerting Protocol (CAP feed), and;

Compliant. We have embedded CAP messaging directly in our alerting interface, making it quick and easy for your notifiers to broadcast CAP activations to trigger other alerting systems and related safety systems. You can easily activate CAP-compliant systems at the same time as other delivery modes like text and emails. We maintain compatibility for the latest CAP standards, currently versions 1.1 and 1.2, and support *both* the CAP Producer role (activating a remote system) as well as the CAP Consumer role (where another system activates Rave Alert).

Our tools are flexible and customizable to any CAP-compliant system, so your administrators can set Rave Alert to trigger different siren sounds, broadcast specific content to digital signage, and interface with radios, depending on the capabilities of your other systems. Alert Authors can select collections of CAP settings with one click, keeping alerting simple and efficient, and CAP-enabled channels receive both short and long messaging content to support more flexible system behaviors.

CAP feeds from other systems can also automatically activate Rave Alert based on filters you decide. For example, you can set Rave Alert to automatically message specific groups about incoming weather warnings from the National Weather Service. You can choose which weather situations activate Rave Alert, which recipient groups receive the automatic alert, and how Rave Alert automatically generates a message based on the CAP document.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

TTY for hearing impaired.

Compliant. Rave Alert automatically detects TTY/TDD devices and provides messages in the proper format for them.

If bidder supports additional channels not listed above, please list them in the space provided below.

With Rave Alert, you launch any available delivery modes to any combination of recipient lists, all through one simple interface.

Rave Alert can send through:

- **Text/SMS (over SMPP)** - recipients open 90% of SMS messages within 3 minutes
- **Email** - clearly identify your alerts with custom from: and reply-to: addresses and HTML formatting
- **Voice calls** - ensure recipients pick up the phone with custom caller-id and recordings, and gather your emergency response team quickly with automated conference call-bridging
- **RSS feed** - trigger digital signage, sirens, websites, and more
- **Social networking sites** - reach community recipients without any contact information through Facebook and Twitter
- **Common Alerting Protocol (CAP)** integrated platforms - integrate with your other alerting systems like digital signage, PA systems, sirens, and send automatic weather notifications from the National Weather Service (NWS)
- **Integrations** - send desktop alerts and activate on premise technology through Alertus and launch alerts directly through your incident management platform through integration with Juvare's WebEOC
- **IPAWS messages** - Includes support for WEA 2.0, IPAWS 3.0/3.1, and the IPAWS Labs Cloud test environments
- **Mobile applications** - Target users based on real-time location with push notifications and rich content.
- Alphanumeric pagers, and more

Many of the modes of delivery to end users are listed above; however, Rave has a few other ways to get messages delivered to all registered users in the system including:

1. **Voice- and/or DTMF- initiated integrations**. Utilizing Rave Alert's voice calling and extension management features, several customers have integrated Rave Alert with PA systems, blue box broadcast and more.
2. **Text gateways:** Numerous systems support gateway clients that can trigger system events.
3. **Direct integration**: Rave's two Application Programming Interfaces (APIs) can be used to extend access to rich product functionality directly from remote systems via standard web services. These may include firing alerts from a remote hardware system's client programmatically, as well as the building of customized interfaces and remote provisioning of

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

subscriber data in real-time. In addition, our web services also provide ways to send individual messages directly from within bespoke applications.

4. **Alertus, Inc**. Rave Alert supports a very deep integration with technology from Alertus, Inc, including the ability to query delivery groups from the Alertus system, configure custom messages and durations, and more

		Yes	3rd Party	Next Release	No
1.2	The EMNS must have a minimum of two (2) geographically separated hosting data center locations by at least 250 miles apart. Both locations must be fully stand-alone, and provide true calling redundancy, and must have the capability to access a minimum of two (2) geographically separated locations by at least 250 miles alternate call server locations, with onsite redundancy per each system. The system shall not require the State to purchase of any additional hardware and/or software. Also, list all your data center compliance and certifications such as AICPA SOC 2 and SOC 3, FedRAMP, ISO 27001, etc. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert maintains 2 geo-redundant SOC2-compliant data centers, one in Massachusetts and one in California. We also have 4 geographically dispersed voice call centers. Our centers have redundant servers, power systems, and failover capabilities with each other. If a machine, power grid, or entire data center has an outage, the system automatically fails over to other resources. We replicate data between servers and centers, so no outage can cause a data loss.

These data centers make use of industry-standard safeguards such as 24/7 manned security, facility entry controlled by electronic keycards with pin codes, mantraps, and biometric scanners, locks on all cabinets, cages, and suites, and CCTV monitoring.

Physical access at each facility is controlled with three access safeguards. First, a named access control list identifies the only Rave representatives authorized to access the data center. At the data center, only these authorized personnel can pass the two-factor keycard and biometric control system. Finally, a combination lock secures the cabinets housing Rave's physical servers. This combination key is kept in an encrypted "password safe" accessible only to Rave System Administrators.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

We monitor our servers 24x7 and provide all system maintenance to ensure Rave Alert is reliable, available, and provides high performance.

Please see the attached *Rave Mobile Safety Platform Data Privacy and Security Overview*, appended to this response, for a detailed review of Rave's information security and privacy protections.

The system shall not require the State to purchase of any additional hardware and/or software.

Compliant. Rave Alert is a cloud-hosted platform with no hardware or software components required, other than integrated systems (e.g. by CAP) that the State wishes to maintain on premise.

Also, list all your data center compliance and certifications such as AICPA SOC 2 and SOC 3, FedRAMP, ISO 27001, etc. Describe how the solution will meet this requirement.

SOC2 reports for our data centers are appended to this response. Evaluations are performed in accordance with AICPA Statement on Standards for Attestation Engagements No. 18, "Clarification and Recodification" among other common industry controls and several other critical standards.

In 2019, Rave Mobile Safety has completed all configuration, documentation, and released necessary security enhancements for FedRAMP certification at the Moderate level, and is in the final third-party certification process (3PAO). Finalized certification is expected in early Q2'2020. Once Rave attains our Authorization To Operate (ATO) within the FedRAMP system, Rave's security package will be available on the FedRAMP Marketplace. (Please note that only government and military (those with .gov or .mil email domain addresses) organizations are authorized to access these materials). Also, please note that FedRAMP places certain restrictions on data allowed on the AWS FedRAMP-compliant storage tier used in our Federal compliance environment. Customers deployed on Rave's infrastructure rather than FedRAMP enjoy most of the same protections, controls, industry-standard processes and implementations that are used when Rave Alert is supporting customers in the FedRAMP environment.

GRX, Rave's independent auditing team, utilizes industry best practices and methodologies for penetration testing, such as the OWASP Guide/OWASP Top 10, Open Source Security Testing Methodology Manual (OSSTMM) and National Institute for Standards and Technology (NIST). GRX also is a SANS/GIAC Certified Web Application Penetration Tester. These methodologies and certificated training ensure a complete and consistent approach to the assessment.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Among the specific tools used during Automated Vulnerability Assessments for Rave Alert, Rave and our auditors have used the following tools:

- Burp Suite
- OWASP ZAP
- Fiddler
- Nmap
- Nessus
- SqlMap
- Nikto
- Open Vas

Note: For FedRAMP compliance certifications, some additional or different tools may be used by the 3PAO.

Please see the certification document attached to this response as well as the SOC2 audit compliance certification for Rave's co-location partner, Internap.

BSN003 SOC 2_FINAL 2018.pdf
SJE011 SOC 2_FINAL 2018.pdf
INAP SOC 2 Bridge Letter January 2019.pdf

Note: At the time of this response, the final SOC 2 reports are not yet available for 2019; the INAP SOC 2 Bridge Letter January 2020 provides preliminary results; when available, final versions will be available upon request.

		Yes	3rd Party	Next Release	No
1.3	The EMNS must be available 99.999% of the time. Describe how the solution will meet this requirement.	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave supports a standard 99.999% (aka "five-nines") service availability policies fully detailed in our appended Master License and Services Agreement (MLSA) document. Rave's Public Safety-Grade Infrastructure is built on 15 years of operational experience as a cloud-hosted solutions provider, a platform that sent over 2 billion messages during calendar 2019 and that evaluated over 20% of *all* 9-1-1 calls placed in the United States.

		Yes	3rd Party	Next Release	No
1.4	The EMNS must include 24x7x365 system support, no queue, and no wait customer service/help desk. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Excerpted from our standard support terms in the Rave Master License and Services Agreement (MLSA) appended to this response:

Purpose.This service level policy sets forth Rave's undertakings with respect to providing customer support to the Client and the service levels associated with the Services provided to Client during the Term of the Agreement.

Service Reliability. Rave shall provide an uptime of 99.999% for the Services, subject to scheduled updates and scheduled maintenance and to any downtime caused by the Client or by Third Party Service Providers. For unplanned downtime an "Event", Rave will assign a trouble severity code based on Rave's assessment of the Event at the point of trouble identification. Rave will make adjustments to the trouble severity code based on how the Event proceeds.

Trouble Severity Code	Description	Initial Response Time	Status Update Intervals
Sev 1	"Sev 1 Error" means a catastrophic Event causing a complete 100% loss of a key safety related feature of the Services	20 min.	30 min.
Sev 2	"Sev 2 Error" means a non-catastrophic Event causing a significant component of the Services to fail or to perform	For Events reported during normal business hours 9am to 5pm EST Monday through Friday, 24 hours	2 hour

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

	materially different than expected, creating significant inconvenience to the Client	from time of report. For Events reported outside of normal business hours, 24 hours from beginning of next business day		
Sev 3	"Sev 3 Error" means an Event that: a has minimal current impact on the Client, and b causes a malfunction of a non-essential Product feature.	For Events reported during normal business hours, 24 hours from time of report. For Events reported outside of normal business hours, 24 hours from beginning of next business day	As appropriate	

		Yes	3rd Party	Next Release	No
1.5	The EMNS must ensure that the database is PII compliant. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant.

The typical core emergency notification contact information stored in our systems is typically classified as "directory data" rather than PII. Social security numbers and e-commerce information are never stored in the system. Where appropriate, our controls are based on NIST 800-53 version 4 controls.

Rave Mobile Safety maintains its own database and bespoke operational and applications infrastructure hosted in geo-redundant co-location facilities in Santa Clara, CA and the Boston, MA areas.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
1.6	System upgrades and security patches for the EMNS must be provided at no additional cost to the State. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Mobile Safety provides all upgrades and system maintenance at no additional cost.

		Yes	3rd Party	Next Release	No
1.7	The EMNS must be capable of being securely accessed by designated division administrators for initiation via any and all of the methods listed below. Please describe how the system can be accessed for notification initiation. a. Any internet access connection, including dial-up or satellite without any additional software; b. Telephone Live support with no waiting cue; c. Email; d. Mobile device apps.	Yes			

Bidder Response:

Compliant. Your administrators access Rave Alert through a secure, mobile-friendly website that can be accessed from any device with internet connection. Our interfaces are mobile-responsive, so they automatically size to any device, including computers, mobile phones, MDTs, tablets running iOS, Android, and other mobile OS.

Perhaps most important, Role-Based Access Controls (RBAC) features (described in detail in surrounding responses) ensure safe and secure access permissions and system scope are supported properly for occasional users, sub-jurisdictional communications, and other scenarios where permissions need to distributed or delegated permissions for divisional administrators.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Figure: Send alerts from any Internet-enabled device, including desktop and laptop computers, iOS and Android mobile and tablet devices, Windows mobile, and more.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

We test against the current version and one version back of:

- Google Chrome
- Mozilla Firefox
- Apple Safari
- Microsoft Edge
- Microsoft Internet Explorer (current version only)
- Mobile browser versions on iOS, Android, and Windows Phone

The interface maintains the same structure regardless of device, browser, or location, so even if they have to access the system from a different device your administrators can quickly navigate the familiar interface.

Telephone Live support with no waiting queue;

Compliant. Please see our Severity prioritization system documented in our MLSA documentation and contracting instruments, and shown above in prior responses.

Email;

Email support processes are tied directly to Rave's Technical Support ticketing systems. Ticket histories on all support incidents are available within Rave Alert's support pages; these appear via a "Help" link on every screen of the product.

Mobile device apps.

Compliant. Using standard product interfaces and relevant support features.

		Yes	3rd Party	Next Release	No
1.8	The system must support the establishment of multiple notification subdivisions/groups for each division or jurisdiction. Describe how the solution will meet this requirement.	Yes			

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Bidder Response:

Compliant. Several responses have detailed our group and list management features, and the wide range of options that include automated lists of different types, several flavors of manually-created and *ad hoc* lists, dynamic lists that target attribute tags set as user properties (e.g., division, department, location, user role, etc.), lists from data sources, and opt-in lists managed on self-service portals, in mobile apps, or by optionla SMS Opt-in Keyword affiliations.

List automation tools combine with roles and RBAC permissions in Rave Alert to support distributed management of lists as well. Lists become a vehicle for accurate segmentation of recipients, but also a natural and intelligible mechanism to determine which recipients activators in a given role can manage and send messages.

		Yes	3rd Party	Next Release	No
1.9	The EMNS must allow individual administrators and recipients to designate multiple devices to receive notifications. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Rave provides both a public portal and mobile application where residents, commuters, and businesses can add and update contact information.

Through both interfaces different alert categories can be chosen based on the registrant's location, allowing you to intelligently support both resident and commuter populations. Community members can input **unlimited contact numbers**, including wireless devices. Information that your community members put on this portal is updated in real-time on the system and available for use immediately. You can configure different opt-in subgroups for your users to choose from. Users can choose what type of alerts to receive, and what devices to receive them on.

Staff and similar "internal" user accounts support 10 contacts per subscriber. Rave supports an independent self-service portal experience for public users and private staff and other privileged user accounts. This minimizes risk and avoids confusion between jurisdictional business users and residents/citizen subscribers. When jurisdiction staff also maintain public accounts, Rave Alert

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

automatically de-duplicates redundant data down to the individual contact details to support a single message per device for all recipients.

		Yes	3rd Party	Next Release	No
1.10	The EMNS must permit recipients to respond immediately on any two-way device (phone, mobile device or email) as well as provide a call back response number for one-way devices like fax machines and one-way pagers. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert supports two-way messaging, allowing responses to text and voice messages that are collected in standard reports, with an active notification of receipt sent to the sending admin. Rave Alert generalizes this functionality by use models that take advantage of our multi-modal response support.

Rave Alert email profiles, for example, allow selective routing of responses to specific mail accounts or mail servers; SMS responses are supported via 2-way SMS capabilities; voice responses are managed via an easy to apply preset configuration. Rave Alert has been used in numerous jurisdictions for callouts - police, fire and EMS responders, EOC activation teams, SWAT teams, volunteer callouts and more.

User Confirmation and Account Verification

As noted, Rave Alert also supports a range of user confirmation processes, each tuned to specific delivery modes within the construct of a multi-modal alert. Confirmation is available for most delivery modes. Options include SMS replies with full support for 2-way SMS, email replies tied to re-usable "email profiles" that allow customers to input, manage, and store multiple email addresses for replies, and voice response that can confirm receipt or conduct "voice surveys" by soliciting specific touch-tone responses from recipients. Responses are collected in standard reporting and can easily be exported from the system for distribution or management in another system when needed.

Voice Recording / Inbound Call Platform

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

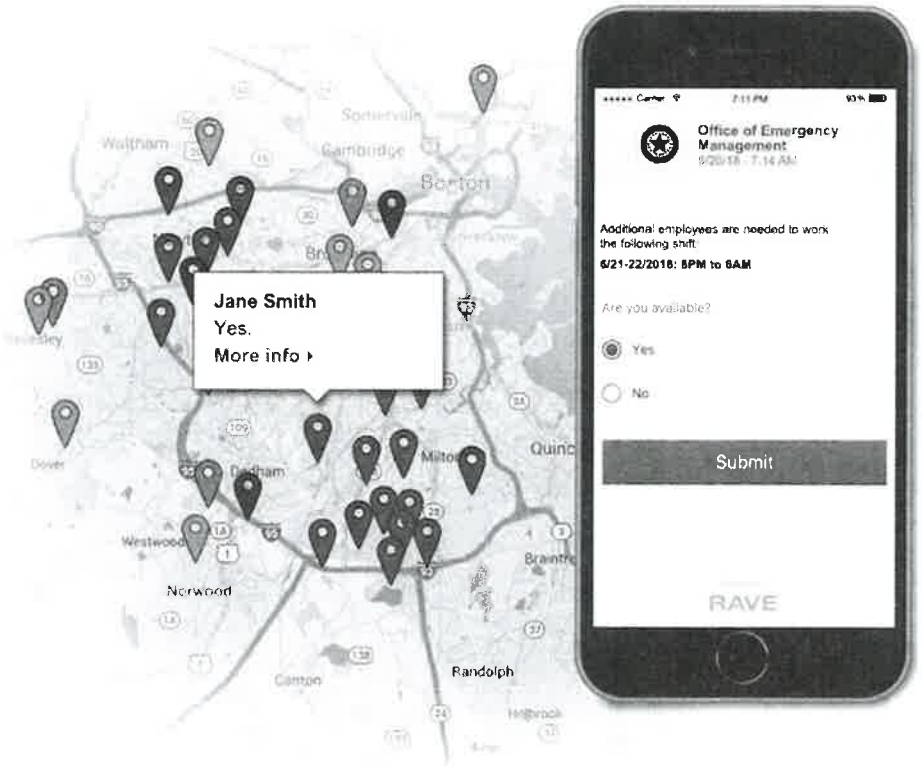
Rave Alert offers an optional Inbound Voice Message service that provides clients with a toll-free inbound number that plays a per-alert configurable recorded voice message. Numbers may be toll-free or local exchanges, with the latter featuring a fully customized Caller ID label. Inbound Voice services use Rave Mobile Safety's large service capacity to deliver the message to thousands of incoming callers, avoiding congestion on your local phone lines and emergency services numbers. The inbound number may also be distributed to function as a "hotline" number for public information when needed. When configured, within Rave Alert voice messaging, a single checkbox sets that recorded hotline as the Caller ID for a voice alert; recipients who hit the "call back" button after missing a message would then be connected directly to this recorded update.

Location-Aware Polling for Check-Ins, Reunification, Callouts and Staffing Needs

Rave Alert also features a Geo-Polling alert type with features allowing you to ask recipients a question and have them choose from set answers you specify.

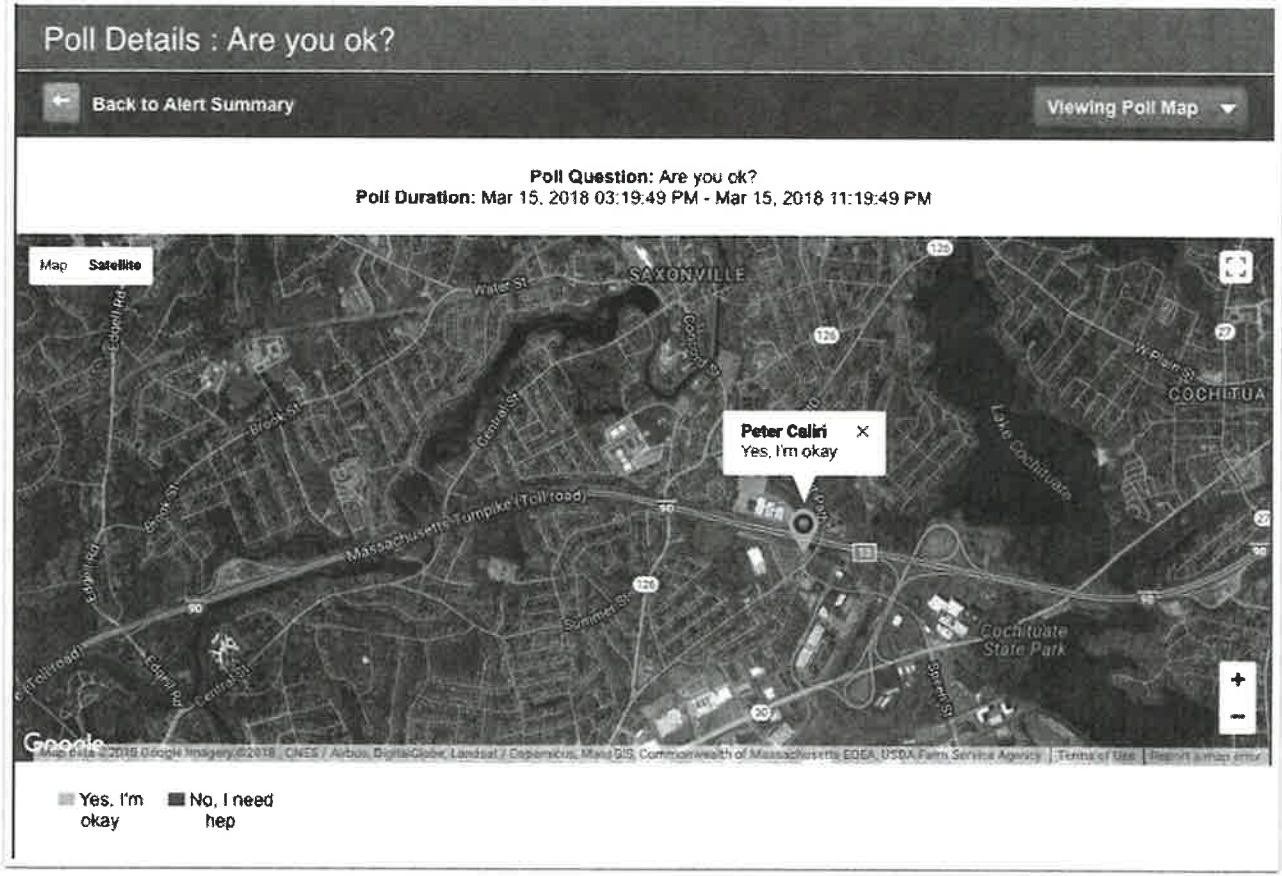
Polls support distribution by SMS, email, and voice call. These polls can be set to expire after a certain time and stop allowing replies from recipients. In addition, a "quota" capability can close a poll after a specific number of responders choose a specific reply.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Most important, poll response collection **does NOT require a mobile application or specific device to receive and respond** with status and to provide optional responder location. Rave Alert generates a dedicated response report for every alert that records responses from any of these tools. For polls, these reports contain graphs, charts, and maps of available answers, as well an export capability for results.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Polls support additional functionality extending our "Follow Up Alert" features, allowing additional messaging to respondents based on response/non-response, or selection of a specific response option.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Optional- Rave EyeWitness

A two-way text messaging platform that increases participation in community policing efforts. Through Eyewitness your community can anonymously or confidentially report crime & safety concerns via text messaging. The Eyewitness program opens up a tip line to any user with an SMS-capable mobile device. Each event in the system is captured for analysis and detailed after-action and trend reporting, with a variety of interactive reporting tools ranging from case history to tip conversations.

		Yes	3rd Party	Next Release	No
1.11	The EMNS must be compliant with all requirements outlined by IPAWS 2.0 and WEA 2.0, including Spanish language and state/local WEA testing. Describe how the solution will meet these requirements. a. Is EMNS capable of allowing a state authority to issue Wireless Emergency Alerts with an event code of CAE (Child Abduction Alert)? b. Does the EMNS meet all critical functions outlined by FEMA in its vendor letters dated February 27, 2015 and May 2018?	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant with recent IPAWS updates include WEA 2.0, IPAWS 3.0 and 3.1 platform releases, and proposed updates to Spanish language character encoding. Rave releases updates to IPAWS functionality within a commercially reasonable period once FEMA makes updates generally available, and will continue to do so as long as features continue to be in sync with customer and industry needs. Rave is committed to ongoing enhancements of IPAWS functionality as new capabilities become available. Rave provides full support for the IPAWS Labs Cloud test environments for required monthly and other tests.

Note that CAE events are supported in the product when FEMA and NEMA have provisioned permission to send in the Event Codes certificated in the jurisdiction's MoA, keystores, and IPAWS certificates.

Does the EMNS meet all critical functions outlined by FEMA in its vendor letters dated February 27, 2015 and May 2018?

Compliant. All capabilities and requirements from the referenced vendor 2015 and 2018 letters are met. When the February 2015 letter was first sent, one Rave customer maintaining a COG sent a letter offering an opinion and complimenting Rave on the quality of our IPAWS functionality, noting that we not only *met* the requirements but deliver a quality user experience while doing so.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
1.12	All EMNS access must be compatible with existing equipment without any modification, reconfiguration or additional hardware. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert is a fully cloud-hosted product. No hardware, software or server components are required at the customer premise.

		Yes	3rd Party	Next Release	No
1.13	The EMNS must allow multiple administrators to make simultaneous outgoing calls. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. There are no practical or significant technical limitations on the number of concurrent users of either administrative or end-user portal interfaces or the number of simultaneous or concurrent active alert campaigns. Rave Alert is architected to ensure to support high volume notifications within your jurisdictions as well as regionally during events impacting many locations and localities. Rave's platform capacities are built to scale; details are elaborated in surrounding responses covering the details of our operational infrastructure.

		Yes	3rd Party	Next Release	No
1.14	The EMNS must have Common Alerting Protocol (CAP) and RSS outputs. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant.

Common Alerting Protocol

We have embedded CAP messaging directly in our alerting interface, making it quick and easy for your notifiers to broadcast CAP activations to trigger other alerting systems and related safety systems. You can easily activate CAP-compliant systems at the

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

same time as other delivery modes like text and emails. We maintain compatibility for the latest CAP standards, currently versions 1.1 and 1.2, and support *both* the CAP Producer role (activating a remote system) as well as the CAP Consumer role (where another system activates Rave Alert).

Our tools are flexible and customizable to any CAP-compliant system, so your administrators can set Rave Alert to trigger different siren sounds, broadcast specific content to digital signage, and interface with radios, depending on the capabilities of your other systems. Alert Authors can select collections of CAP settings with one click, keeping alerting simple and efficient, and CAP-enabled channels receive both short and long messaging content to support more flexible system behaviors.

CAP feeds from other systems can also automatically activate Rave Alert based on filters you decide. For example, you can set Rave Alert to automatically message specific groups about incoming weather warnings from the National Weather Service. You can choose which weather situations activate Rave Alert, which recipient groups receive the automatic alert, and how Rave Alert automatically generates a message based on the CAP document.

RSS Alert Type

Rave Alert supports posts to unlimited RSS feeds. You can assign individual administrators access permissions to specific RSS channels as needed, governing access to RSS alerting modes as a whole or distributing permission to different RSS channels across organizational boundaries.

		Yes	3rd Party	Next Release	No
1.15	The EMNS must have the ability to convert text to speech. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. For each voice alert, you can choose between computer-generated text-to-speech and recording a message. Each alert can use either method, and the customer can choose which method presents as the default, and which the alert author must select to activate. Content of either TTS or voice recorded formats can be pre-saved through the system, or configured at send-time by the alert author as needed.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Text-to-speech synthesis is of very high quality with solid natural language parsing capabilities. The system automatically carries text content from other short-form delivery modes, or you can customize the message for the specific alert.

To record a voice message, the alert author can prompt the system to call any available phone number, and displays the administrator's active devices as selections. You can always preview recorded messages before sending your alert.

Our voice alerts also let you pre-configure an optional recorded preface to voice messages, such as "Please stay tuned for an important message from [your organization]". This type of recording lets you consistently identify your alerts even if you use both text-to-speech and recorded messages.

Alert authors can review recorded messages from the voice alert configuration tools, or from the review message window that always shows before you send an alert.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
1.16	The EMNS must be able to receive multiple responses such as touch-tone signals to initiate further actions. Describe how the solution will meet these requirements. These actions must include: a. Initiate a new notification upon selection of that response; b. Escalate the event upon selection of that response; c. Select a response that must automatically connect to a specific phone number; d. Instantly join a live conference call; e. Transfer the notification to another person if the recipient is unable to respond; If additional responses are available, please list in the space provided below:	Yes			

Bidder Response:

The EMNS must be able to receive multiple responses such as touch-tone signals to initiate further actions. Describe how the solution will meet these requirements. These actions must include:

Initiate a new notification upon selection of that response;

Compliant. Rave supports a "Follow Up Alert" feature. This allows additional messaging to recipients of a previous alert based on required needs. Follow Up Alert allows you to choose a template or create a new alert ad-hoc making it easy to communicate without making additional recipient selections.

Escalate the event upon selection of that response;

Compliant. Managed via workflows for follow up alerting or via features that notify executive and PIO functions to the details of a notification campaign, and by features to notify admins when responses are provided by recipients.

Select a response that must automatically connect to a specific phone number;

Compliant. Bridging feature is a standard function of Rave Alert voice notifications.

Instantly join a live conference call;

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Alert supports this requirement with its Conference Blast™ feature. Conference Blast allows the user to bridge a voice alert recipient directly into a conference bridge hosted on any standard conferencing service used by the customer. Automated PIN code entry is a standard feature that can be enabled on any alert.

Transfer the notification to another person if the recipient is unable to respond;

At this time, requires a manual workflow action to complete.

If additional responses are available, please list in the space provided below:

Compliant. Some additional voice response features and functions are available:

- Voice responses may be collected as message confirmations or as arbitrary "Call Enabled Response" functions where a message prompts the user to choose an option by touch tone.
- The user can optionally choose to be connected to one of our optional inbound call lines to hear a recorded update or other message.
- Rave's Polling Alert type distributes polls and collects responses by any combination of text, email or voice touch-tone response.
- Location-aware polling that can derive location reporting with poll responses.
- Follow up alerting features can target respondents and/or non-respondents as needed.

		Yes	3rd Party	Next Release	No
1.17	The proposed EMNS must not disrupt existing network security already in place, and must operate at a minimum of the 2048bit-key encrypted NSA (National Security Agency) standards. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. As a hosted solution with no significant on-premise technology, our impact on your local systems will not interfere with common network security protocols. During onboarding, Rave's Services teams work to secure your installation and to ensure secure connectivity at any key areas. Rave reaches your systems from 1 of 3 certificated IP connections; data exchange by file is supported over secure configurations such as SFTP with public shared key security. Customers who choose to integrate Rave

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Alert authentication with directory services/identity management/SSO platforms work with Rave to configure secure encrypted connectivity using industry and State IT best practices. Information is encrypted in transit and at rest in all connected systems.

		Yes	3rd Party	Next Release	No
1.18	Selectable access and security must be provided for administrators to control all user functions (Example: one user may be allowed to perform all functions; while others may be limited to performing restricted functions such as access only to update call lists, or only to view notifications in progress but unable to modify or end an alert). Describe how the solution will meet this requirement.	Yes			

Bidder Response:
Compliant. Rave Alert's substantial access control features - a cornerstone of the product - is detailed in response 1.8 above. All specific access-control use cases above, and many more, are supported by Rave's robust RBAC functionality. Assigned roles instantly present a new or updated administrator with a role-specific view into the system focused on practical daily use and clear and correct activation scenarios. Once assigned a role and all its inherited permissions, roles can also be "overridden" to provide individual-specific changes that a given administrator may need in addition to the default set.

When new permissions are added to a role, for example when new templates are added to defaults, all administrators in the role will see the updated functionality immediately.

Rave's RBAC tool provide a rich field to optimize the system for specific use models and to correctly observe divisional boundaries among activator administrators. More, it supports a delegated administration model that richly supports "distributed administration" needs. A simple example would be the ability for a police department or 9-1-1 center user to support sub-teams where each team lead is free to create and manage their own team memberships and permissions, but only within their specified scope of assigned permissions.

Use of these features can then de-centralize some or all of the typical management tasks overseen by a program office, department, alerting authority, sub-team, or other domain-specific administrative functional area. The key principles that make Rave Alert a favorite tool for activators:

1. Hide all functionality that a given administrator should *not* use. Example: IPAWS functions never appear to users who should not use them. Social media access can be suppressed completely - so the activator has no visible option to send a

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Twitter or Facebook update for example - or to selectively present specific accounts to specific admins to maintain boundaries.

2. Since the user sees ***only*** specific features relevant to their use of the system, as permissions are applied, the impact on product workflows is a simplification of the system, making it both easier to use and less error-prone.

		Yes	3rd Party	Next Release	No
1.19	State of Nebraska data must never be sold, transferred, shared, or otherwise used for any other purpose than for explicit use by the EMNS. Likewise, the data must never be reviewed for data harvesting or any other type of metric analysis other than explicitly required for operation of the EMNS. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave does not provide personally identifiable information in any way to telemarketers, analytics firms, or other solicitors. This policy is clearly stated in both contract instruments with the customer as well as Rave's privacy policy.

		Yes	3rd Party	Next Release	No
1.20	State of Nebraska data is the property of the State of Nebraska and remains so throughout the life of the contract to include any and all renewals and/or extensions. All data will be returned immediately at the end of the contract to the State of Nebraska. No copy of the data will be retained by the contractor. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant and provide clear guidelines for data ownership. The customer retains ownership of all employee / staff and end user information. This is documented in our Master Licensing and Services Agreement (MLSA) (appended to this response) and contracting instruments.

Rave maintains a strict privacy policy to protect user information. This policy is stated in both Rave's contracting with the customer as well as Rave's privacy policy. Information input by our customers and collected as part of their alerting remains their property, and will be returned to clients upon termination of the contract. Typically, this includes all content provisioned by staff/employee

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

opt-ins as well as data feeds from enterprise repositories such as ERP or HR systems, as well as data provisioned using self-management tools such as Managed Contacts or manually managed account information.

9-1-1 and similar data source ownership *may* vary for reasons outside of Rave Mobile Safety's control, and may be subject to licensing agreements or contracts among the State and its jurisdictions and specific data providers or public agencies. Information input by individual citizens, such as emergency vulnerabilities and other personal information, remains their property and subject to privacy policies, and will remain their property at the termination of the contract.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

	Message Management Requirements Section 2	Yes	3rd Party	Next Release	No
2.1	A message initiator must have the ability to create and send notifications in under two (2) minutes. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert provides **a single workflow for sending a multi-modal alert**, which carries message content automatically between communication modes, while still allowing mode-specific edits if required. This saves time and effort when creating vital alerts. For example, text-to-speech scripts can be carried from the content of text alerts, and so on.

Emergency messages are not sent every day; when a crisis occurs, or a weather closing at 5am for example, your staff should be focused on the event, not on software. Rave Alert's emphasis on ease of use ensures that your broadcast administrators don't need a software manual every time they need to alert your community. Alerts can be activated in less than 60 seconds using all available modes.

Rave applications can be accessed in several ways:

1. Via standard web browsers listed below.
2. Rave Alert has a fully mobile-responsive user interface that supports access on mobile devices such as smartphones and tablets on any Internet-connected device platform
3. Via live operator, 24x7x365 support hotline in the event that power or connectivity are compromised.

Rave also supports an emergency login feature for customers who tie authentication to LDAP, AD, or SSO servers hosted on the customer's site; if the authentication provider systems are unavailable, administrators can use this emergency login to access the system to send alerts. In the event that all access is limited, for whatever reason, Rave provides 24x7x365 emergency notification support by telephone, where the Rave support team can send a message on behalf of the institution.

All product features are fully exposed through a mobile-responsive user interface that will size itself to smaller device profiles such as smartphones and tablets running iOS, Android, Windows Mobile, and other OS, as well as most ultrabook and netbook computers.

Clients can pre-save message content in unlimited number of templates. Templates allow you to predefine every aspect of an alert,

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

including both recorded voice and mode-specific text content. Template values can be edited at runtime as needed to adjust content. Templates are assignable by permission to control access, and use a very rapid filter/search function. Even without a template saved, however, multi-modal activations can be easily completed in under 2 minutes when message content is ready.

Rave Alert offers an intuitive Admin Console accessible over the web via a mobile-friendly, encrypted web site. This means Rave Alert's Admin Console will size to any internet-enabled device, from computers to smartphones, tablets running iOS, Android, and Blackberry OS, and most netbook and ultrabook computers.

Rave's customers praise the product's ease of use: Rave Alert provides a guided workflow, mobile responsive design, and customizable permissions that simplify the user interface for alert authors. These features combine to provide simple, effective alert construction and broadcast to our customers regardless of location and stressful conditions.

A Tested and Proven User Experience Designed By Our Customers
One size does not fit all. Rave Alert's interfaces are wholly customizable and surface features to each admin based on individual and role-based permissions.

One example is Rave Alert's specially configured SnapSend™ interface for the fastest possible alert sending process. In a simplified view the alert author signs in and selects a template from a list of templates assigned to them. This may be 1 or 2 specific templates, or many, as required: A selected template is populated for multi-modal distribution. In this specific configuration, the alert author provides both a short message for appropriate short modes such as text message, Twitter, and others, and a longer message (if needed) that contains more details for email and other longer delivery modes. This model is designed for a "type words and go" methodology. Rave Alert automatically broadcasts the appropriate short or long message for each enabled delivery method. SnapSend allows alert authors to edit just words, and then confirm the message delivering it by many mechanisms.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Rave's unique SnapSend™ feature provides a managed template for alert authors who require the simplest and most efficient messaging workflow.

Many usability experts attest that designing for simplicity is a complex and difficult task. Rave Mobile Safety used 15 years of experience and a year-long consultation with its customer advisors to produce this simplified of workflow. A picture does not do its interactivity full justice.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Most importantly, this workflow is **one choice among many**, and may be perfect for some users but not optimal for others. Rave Alert supports robust customization to allow your interfaces to support many uses (mass notification, departmental notifications, agency public and private notifications for example), and many administrators with varying levels of computer sophistication, with a system that ensures users will not make mistakes or send messages to segments of the community they should not be able to reach.

The product's customizable and easy-to-use interfaces are best experienced in a live demonstration. AT&T and Rave Mobile Safety would welcome an opportunity to demonstrate, rather than just describe, how quickly an alert can be authored and sent.

All administrators must be required to have a user name and password and a role description defining their scope of authority, division, and limits. Describe how the solution will meet this requirement.

Compliant. (Description repeated from Section 1.8 above.) Rave supports best practices focused on using roles to fully render all such administrative permissions closely tied to recognizable naming conventions that represent each roles scope and purpose. We offer customizable permission levels so you can adjust and assign access to different Rave Alert tools in ways that match your current organizational structures and emergency management procedures.

Rave Alert supports standard roles with defined and distributed permissions, and you can create **custom roles** to configure access to nearly every product feature and every delivery mode in your system. You can stipulate, for example, administrators' read-only or read-write access to subscriber data, their ability to create or edit groups, save templates, manage alert distribution lists, and much more. The interface will only show your administrators tools they can use, simplifying the system for people who need to quickly send alerts without distractions, and supporting distributed administration models within your organization. This enhances both ease of use and organizational security.

Custom roles can also control access to specific data objects within the system, for example:

- Selective access to recipient groups (with or without create and save permissions)
- Selective access to individual alert templates (with or without create and save permissions)
- Selective access to delivery modes such as text, voice, email, and social media, as well as integrated systems such as sirens, IPAWS, and digital signage
- Selective access to specific social network pages or accounts on Facebook or Twitter
- Selective access to website feeds, e.g., where administrators at one location should only publish to specific websites

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

- Selective access to profiles that function as presets for *branding and administrative settings* such as Caller IDs on voice calls and email header and footer content
- Selective access to the Shape Library shapes available in the system
- Selective access to reporting features
- Selective access to a range of tools for managing subscriber data
- Selective access to Rave Prepare functions supporting emergency management decision making
- Selective access to system administration and related configuration settings

Rave Alert includes several default administrative roles:

- **Domain Administrator** - A Super User who can access all product features, manage user data, configure the product, and assign administrative roles.
- **Broadcast Alert Administrator** - An Alert author who can send broadcast alerts and view relevant reporting on those alerts. Broadcast Alert Admins view a very clean interface with few tools, supporting limited or occasional use. This admin cannot edit or access subscriber data attributes, improving both site security and compliance with FERPA and other privacy standards. To simplify the interface further, you can limit a Broadcast Alert Administrator to choosing from pre-configured alert templates.
- **List Administrator** -- An alert author who can send broadcast alerts only to specific user lists, and view reporting based on those alerts. You can assign any number of lists to a List Admin, but they cannot message users outside of these lists. Limited permissions like this can address a wide variety of authorization requirements and departmental situations. To simplify the user experience further, you can limit a Broadcast Alert Administrator to choosing from pre-configured alert templates.
- **Managed Contact** - A managed contact is a general role for subscribers flagged as "guest" users - users added via *ad hoc* spreadsheet upload, often covering contractors, interns, food services or other facilities contractors, affiliated agency contacts - users who are not typically stored in enterprise directories, but who are important to your organizations and who need to receive your communications.
- **User** - Standard subscriber role for message recipients.

You can create unlimited administrators, and assign unlimited administrators to each role, default or custom, at no additional charge. We provide on-going web-based training options for all administrators.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

When an administrator/activator is assigned an RBAC role, the user is instantly assigned feature permissions, specific objects such as templates, subscriber lists, accounts and profiles, all from a single assignment. These powerful tools make for a safer system that removes functionality not appropriate to users in roles and at the same time simplifies activations by showing only relevant features.

		Yes	3rd Party	Next Release	No
2.2	All administrators must be required to have a user name and password and a role description defining their scope of authority, division, and limits. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. (Description repeated from Section 1.8 above.) Rave supports best practices focused on using roles to fully render all such administrative permissions closely tied to recognizable naming conventions that represent each roles scope and purpose. We offer customizable permission levels so you can adjust and assign access to different Rave Alert tools in ways that match your current organizational structures and emergency management procedures.

Rave Alert supports standard roles with defined and distributed permissions, and you can create **custom roles** to configure access to nearly every product feature and every delivery mode in your system. You can stipulate, for example, administrators' read-only or read-write access to subscriber data, their ability to create or edit groups, save templates, manage alert distribution lists, and much more. The interface will only show your administrators tools they can use, simplifying the system for people who need to quickly send alerts without distractions, and supporting distributed administration models within your organization. This enhances both ease of use and organizational security.

Custom roles can also control access to specific data objects within the system, for example:

- Selective access to **recipient groups** (with or without create and save permissions)
- Selective access to **individual alert templates** (with or without create and save permissions)
- Selective access to **delivery modes** such as text, voice, email, and social media, as well as **integrated systems** such as sirens, IPAWS, and digital signage
- Selective access to **specific social network pages or accounts** on Facebook or Twitter
- Selective access to **website feeds**, e.g., where administrators at one location should only publish to specific websites

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

- Selective access to **profiles** that function as presets for *branding and administrative settings* such as Caller IDs on voice calls and email header and footer content
- Selective access to the **Shape Library** shapes available in the system
- Selective access to **reporting features**
- Selective access to a range of tools for managing **subscriber data**
- Selective access to **Rave Prepare** functions supporting emergency management decision making
- Selective access to **system administration** and related configuration settings

Rave Alert includes several default administrative roles:

- **Domain Administrator** - A Super User who can access all product features, manage user data, configure the product, and assign administrative roles.
- **Broadcast Alert Administrator** - An Alert author who can send broadcast alerts and view relevant reporting on those alerts. Broadcast Alert Admins view a very clean interface with few tools, supporting limited or occasional use. This admin cannot edit or access subscriber data attributes, improving both site security and compliance with FERPA and other privacy standards. To simplify the interface further, you can limit a Broadcast Alert Administrator to choosing from pre-configured alert templates.
- **List Administrator** -- An alert author who can send broadcast alerts only to specific user lists, and view reporting based on those alerts. You can assign any number of lists to a List Admin, but they cannot message users outside of these lists. Limited permissions like this can address a wide variety of authorization requirements and departmental situations. To simplify the user experience further, you can limit a Broadcast Alert Administrator to choosing from pre-configured alert templates.
- **Managed Contact** - A managed contact is a general role for subscribers flagged as "guest" users - users added via *ad hoc* spreadsheet upload, often covering contractors, interns, food services or other facilities contractors, affiliated agency contacts - users who are not typically stored in enterprise directories, but who are important to your organizations and who need to receive your communications.
- **User** - Standard subscriber role for message recipients.

You can create unlimited administrators, and assign unlimited administrators to each role, default or custom, at no additional charge. We provide on-going web-based training options for all administrators.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

When an administrator/activator is assigned an RBAC role, the user is instantly assigned feature permissions, specific objects such as templates, subscriber lists, accounts and profiles, all from a single assignment. These powerful tools make for a safer system that removes functionality not appropriate to users in roles and at the same time simplifies activations by showing only relevant features.

		Yes	3rd Party	Next Release	No
2.3	The EMNS must allow message initiator to send notifications to an unlimited number of recipients. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert is licensed for unlimited messaging, and there are no practical technical limitations on recipients selected for notifications.

		Yes	3rd Party	Next Release	No
2.4	The EMNS must allow designated division administrators to send pre-scripted or ad hoc emergency action messages using a web-based interface. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

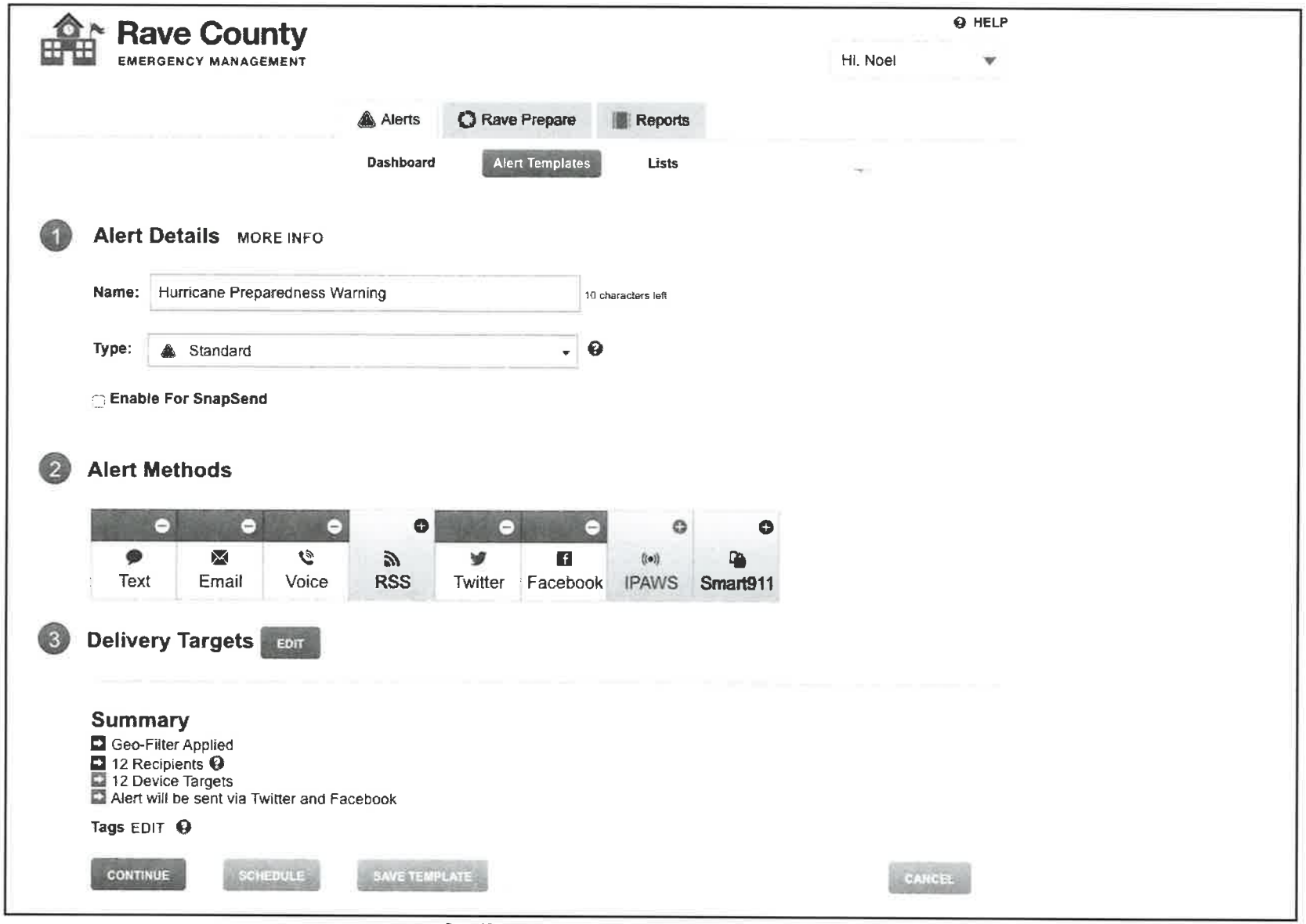
Compliant. Rave Alert supports multiple and customizable workflows that provide several options for both scripted and *ad hoc* notifications. Notification templates are simple to create and even simpler to activate when storing a ready message - 3 clicks to completion, including full message confirmation. While it is easiest to show this simplicity in an interactive demonstration, there are numerous features that speed up both scripted and *ad hoc* multi-modal messages even when starting from scratch with a new message.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Rave Alert features an alert type called SnapSend™ described in prior responses. SnapSend is based on the idea of letting an underlying template determine the mapping of a simple short, and optional longer message, sending each to the appropriately configured delivery modes.

In our standard mode alerts, the user is instead guided through an easy-to-follow 3-step wizard to complete activation:

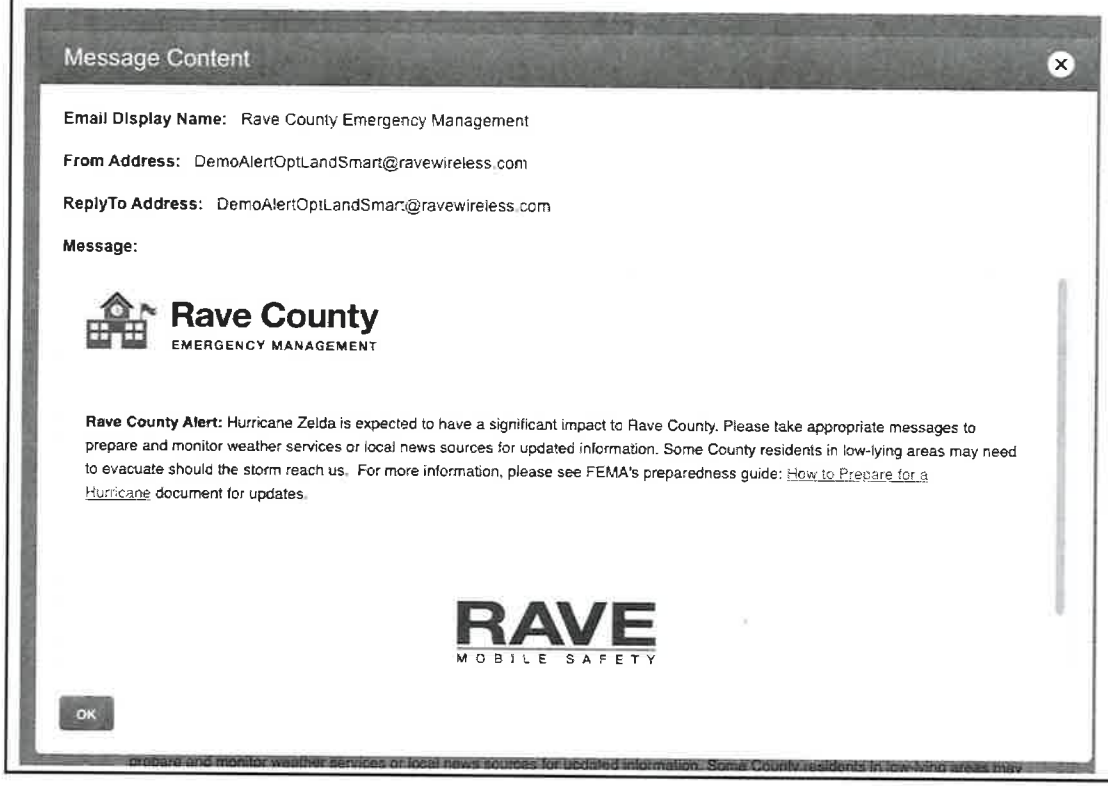
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

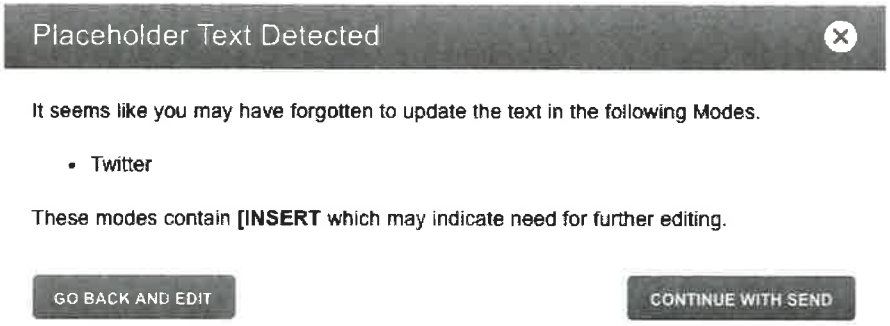
Step 1 names the alert. Step 2 expands to provide the content for each delivery mode, auto-completed by preset "profiles" that automatically configure your preferred settings, and using prior messaging content as a starting message for each enabled delivery mode. Step 3 is where delivery recipients and map-based selections are configured.

Inside delivery modes, features such as our Email Profiles support instant branding of messages and live preview:



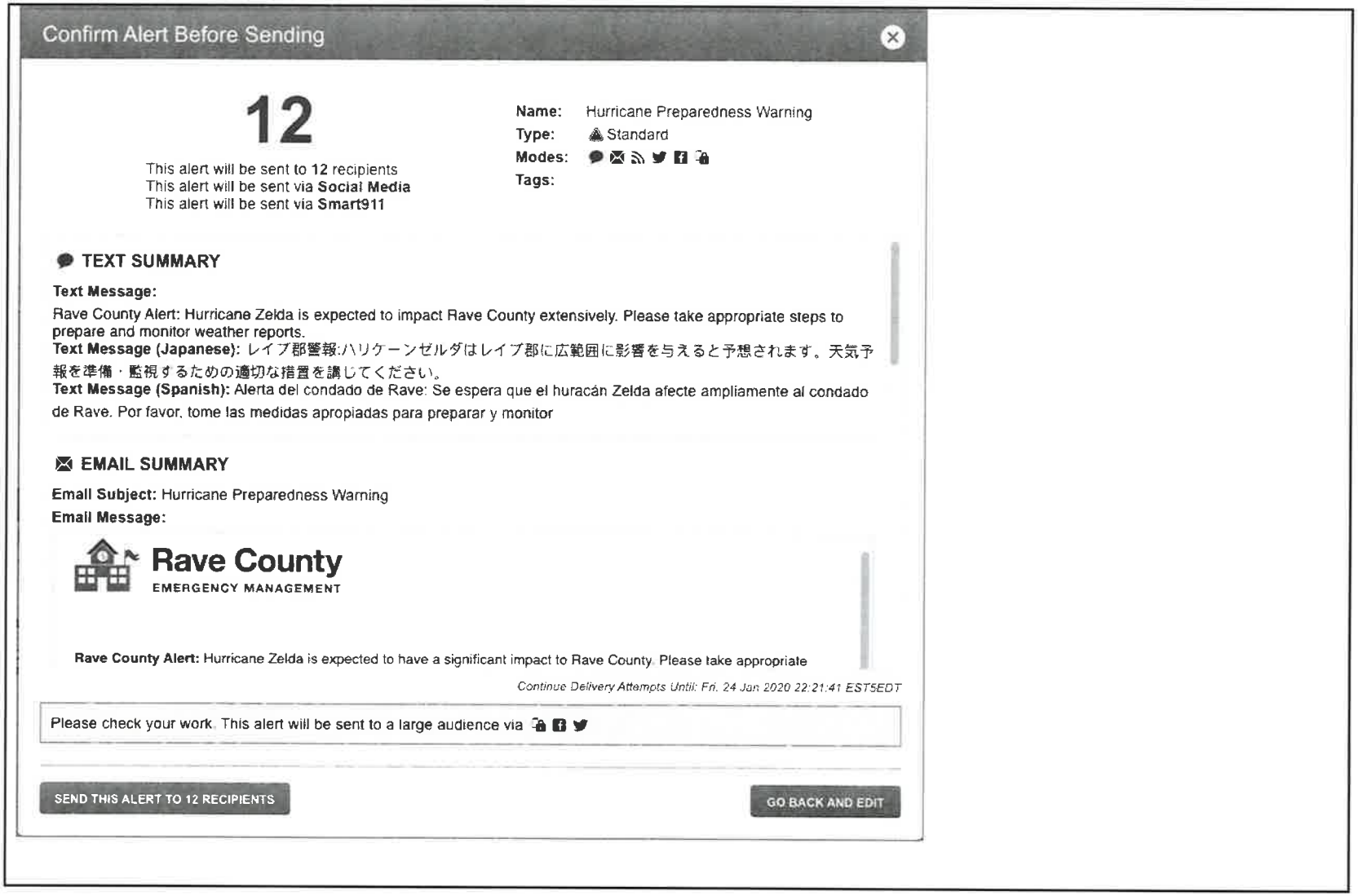
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Another helpful feature for activators: Rave Alert includes a popular feature called "Template Protection" that warns senders when a message contains incomplete details for content within a template - preventing "accidents" where a message has not had the requested data changed in any or all delivery modes when the activator is expected to provide additional details for a notification, ensuring complete messages are sent.



Finally, a critical component to ensuring messages are correct and complete and to reassure activators, Rave Alert provides significant details in a final confirmation step before sending:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
2.5	Message initiators must be able to contact the notification service through a designated website or through a toll-free telephone number to a 24/7 operations center maintained by the contractor. It must be possible to immediately speak with an operator who can: a. Follow instructions to initiate an alert; b. Determine the scope of authority, division, and limits of the caller. Describe how the solution will meet these requirements.	Yes			

Bidder Response:

Follow instructions to initiate an alert;

Compliant. Standard processes supported via our 24 x 7 support hotline.

Determine the scope of authority, division, and limits of the caller.

Compliant. Standard processes supported via our 24 x 7 support hotline include validation of user identity. When requesting assistance, support techs will use an escalation process via established escalation contacts collected during onboarding in the event a caller attempts to utilize features outside the configured access controls for the caller.

Describe how the solution will meet these requirements.

We provide a 24x7x365 technical support line where a Rave support employee can create and send notifications on behalf of clients experiencing messaging issues. We also provide phone and email support for other issues. Our trained support technicians can remotely access your instance of the system to troubleshoot, remotely activate alerts when you have connection issues, or perform other support functions.

We pride ourselves on swift response times and invite you to consult with our references about our past responsiveness. All customer support is handled by domestically located Rave Mobile Safety employees who are trained in system usage, behavior, and security policies.

This support is an included service in the purchase of Rave Alert, and so is available so long as you are within contract for the product. Please see our MLSA documentation for more detailed service terms.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

		Yes	3rd Party	Next Release	No
2.6	The EMNS must include multiple methods to initiate messages. The message initiator must be able to: a. Dictate a message to an operator; b. Record a voice message by telephone or Internet; c. Type a text message using an Internet or a telephone text-messaging device; d. Live operators or the system software must be able to convert text messages to highly intelligible speech. Describe how the solution will meet these requirements.	Yes			

Bidder Response:

Dictate a message to an operator;

Compliant. Via our 24 x 7 support hotline.

Record a voice message by telephone or Internet;

Compliant. Rave Alert allows each voice alert to be generated by recording a voice message or by converting text to speech. Clients can choose which option initially opens as the default, and which administrators must select before using.

Rave Mobile Safety also provides a unique "Call-me" feature for voice recordings, where the system will call an administrator's phone, selected from a list of the sender's active devices, or the administrator may also choose to call the system number to record the message.

Type a text message using an Internet or a telephone text-messaging device;

Compliant.

Live operators or the system software must be able to convert text messages to highly intelligible speech.

Compliant.

Describe how the solution will meet these requirements.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

For each voice alert, you can choose between computer-generated text-to-speech and recording a message via a user-friendly "Call Me" feature. Each alert can use either method and the customer can choose which method is set as the default for each new alert template. To record a voice message, the alert author can prompt the system to "Call Me" at any available phone number.

Text-to-speech synthesis is of very high quality with solid natural language parsing capabilities. The system automatically carries text content from other short-form delivery modes, or you can customize the message for the specific alert. Alert authors can review recorded messages from the voice alert configuration.

Text-to-speech pronunciations can also be corrected within the product's configuration screens; in the event that a specific word, acronym, or name is mispronounced by the system, you can easily adjust the pronunciation to correct it.

Also supported is an "introductory voice" feature that prefixes a recorded greeting before delivering a text-to-speech or other recorded message. This is configurable by alert, with a value stored in alert templates or changed on the fly during alert activation. An example is "This is an official announcement from the State of Nebraska Office of Emergency Management" before then playing a text-to-speech or recording message. This helps identify an official message from the jurisdiction as well as allowing a degree of fine-tuning on the tonality to the notification.

		Yes	3rd Party	Next Release	No
2.7	The EMNS must have the ability to issue multiple notifications modes simultaneously with a single action. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. As noted and illustrated in response 2.4 above, our workflows enable your activators to send multi-modal notifications from a single activation.

		Yes	3rd Party	Next Release	No
2.8	The message initiator must have the ability to define the duration of the notification. (Example: after one hour of attempts to contact recipients the notification must be terminated). Describe how the solution will meet this requirement.	Yes			

Bidder Response:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Overall alert expiration time for all alert delivery modes can be set for any alert or template. In addition, certain delivery modes may have specific settings that offer finer grained control; for example, Polling Alerts can be tuned to expire with the alert expiration, any arbitrary duration up to 60 days, or when a quota of respondents select a specific option a specific number of times. Voice notifications can be configured for a specific count of retries for numbers busy or not answered. IPAWS messages allow you to set timings for Effective and Onset times as well as alert duration. The product also features an alert cancellation command that will immediately shut down communications via all modes in the appropriate fashion.

		Yes	3rd Party	Next Release	No
2.9	The EMNS must include a series of web based, pre-defined templates for emergency messages which administrators can use to initiate messages or can modify or define new ones. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Standard template features support a wide range of messaging needs. In addition, new templates are created from scratch in 1-2 minutes and existing templates may be copied and specialized by a single click functioning much like a "Save As..." command. The solution also includes a library of best practice template content and examples.

		Yes	3rd Party	Next Release	No
2.10	The system must allow for unlimited notifications to be created and stored for immediate activation with the ability to quickly edit notifications ad hoc. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Again, workflow samples and screen captures are provided in response 2.4 above. The user can simply open a template, confirm content and send, or may choose to modify contents as needed. A special feature ensures that messages where the activator is expected to supply specific incident messaging, our Template Protection feature helps ensure activators review incomplete alerts where such information has not been updated in your templates. These features support a very wide range of template use models. In addition, access permissions can be applied to control whether specific administrators can save and create new templates or may only modify existing templates that are defined as standard.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
2.11	The message initiator must have the ability to define the type of message (broadcast, first response, round robin, etc.) and the frequency of calling recipients' devices. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. A wide range of settings and workflows combine to provide appropriate messaging to selected recipients using a range of device targets, opt-in choices, type of notification (broadcast, narrowcast/operational, polling, etc) and default alert expiration across all modes as well as within specific delivery mode settings when appropriate. Under Voice messaging, for example, a specific count of retry attempts for busy and not-answered contact can be configured by alert: how many tirmes to retry such a number and the interval to wait between retries. These settings are combined in Voice Profiles for instantaneous settings - retry features as noted, as well as Caller ID, number of times to play the message, and/or whether to use our Conference Blast feature on any configured voice conferencing service. All Voice Profile settings may also be overridden while reviewing and sending alerts. Other delivery modes, such as CAP notifications, can be sent with default or overridden onset, effective, and duration time settings individually if needed.

		Yes	3rd Party	Next Release	No
2.12	The EMNS user interface must allow for: a. The simple creation of notifications; b. The selection of notification recipients or groups and; c. The ability to edit any portion of the notification prior to sending. Describe how the solution will meet these requirements.	Yes			

Bidder Response:

The simple creation of notifications;

Compliant.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

The selection of notification recipients or groups and;

Compliant.

The ability to edit any portion of the notification prior to sending.

Compliant.

Describe how the solution will meet these requirements.

Compliant. We designed, tested, and revised our interfaces to be easy to use. Through our alert creation process, you can intuitively create configure and send many delivery modes through a single alert. Our interfaces are mobile-friendly, meaning your administrators can use the same simple interface from any internet-enabled device, from computers to smartphones, tablets running iOS, Android, and other mobile OS, and most netbook and ultrabook computers. In addition, the interface meets all stated requirements with elegance:

1. Simple, rapid and effective activations even when starting "from scratch" creating a new message with multiple delivery modes selected.
2. The ability to select recipient groups from among opt-ins, manual, dynamic, automated and other lists from data sources.
3. Similarly, all content selected for active delivery modes may be easily modified before sending. Rave's Template Protection feature also helps ensure that content areas where activators are expected to insert or modify details is completed before sending a notification.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

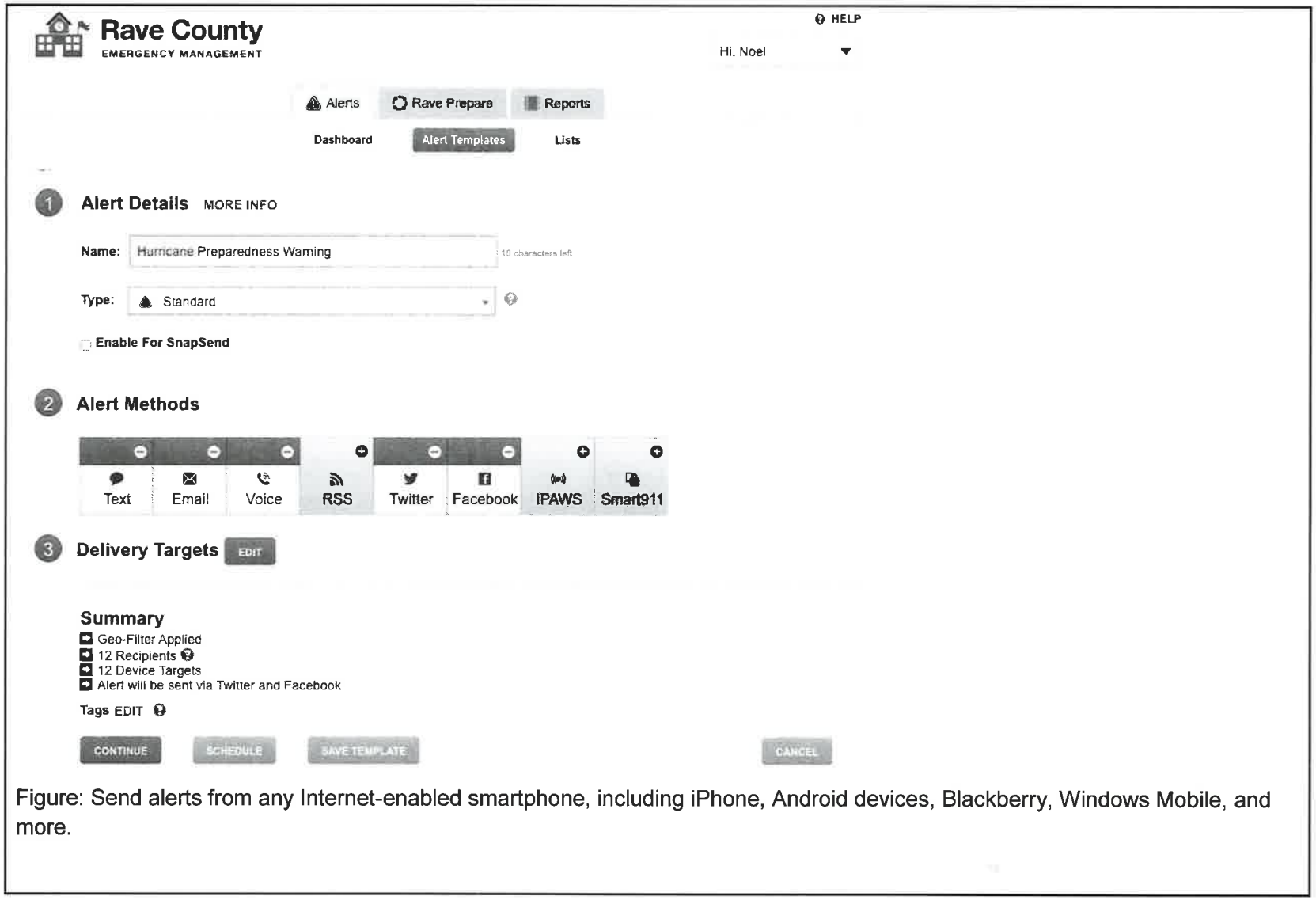


Figure: Send alerts from any Internet-enabled smartphone, including iPhone, Android devices, Blackberry, Windows Mobile, and more.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

We design our notification solution to be simple to use in stressful or distracted circumstances, and work to proactively improve Rave Alert's intuitiveness and ease-of-use based on customer feedback and usability testing. We especially designed our send-flow to make sure even new or unfamiliar users can intuitively follow the send process in emergencies.

A Tested and Proven User Experience Designed By Our Customers

One size does not fit all, and your administrators need to send alerts in different situations and frequencies. We provide tools so you can customize Rave Alert's interfaces to different administrators, only showing specific tools and options based on their needs.

For example, you can assign our simplest SnapSend interface to administrators who only need to send messages as easily as possible. In this simplified view, your alert authors select a template and input a short and long message, which Rave Alert then automatically maps to multiple delivery paths in an underlying template. This provides an easy "type and go" experience, embedding Rave Alert's full power behind the scenes.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
2.13	Message initiator must be able to have scheduled scenarios automatically delivered based on day of month or time of day, where scheduled call-outs can be classified as a recurring activity (Examples: monthly system tests, bi-weekly event postings). Describe how the solution will meet this requirement.	Yes			
Bidder Response: Compliant. Standard scheduling features include the ability to schedule an unlimited number of alerts.					

		Yes	3rd Party	Next Release	No
2.14	The EMNS must have the capability to transmit pre-recorded voice messages or ad hoc messages of any length between 10 seconds and three minutes. Describe how the solution will meet this requirement.	Yes			
Bidder Response: Compliant. There is no technical limitation imposed on voice message length. Text-to-speech notifications are validated to 3,000 characters, which will typically produce a message between 7 and 10 minutes in length.					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution. AT&T Business

		Yes	3rd Party	Next Release	No
2.15	The EMNS must allow the notification to provide recipients with response options that must immediately connect them to an administrator-defined phone number, such as a Service Desk or conference call bridge. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert supports this requirement with its Conference Blast™ feature. Conference Blast allows the user to bridge a voice alert recipient directly into a conference bridge hosted on any standard conferencing service used by the customer. Automated PIN code entry is a standard feature. Any number of conference bridge lines may be configured in Voice Profiles for instant selection during *ad hoc* notifications or when editing a template.

Bridging features can connect users directly to a hotline or other number you wish. In addition, Caller ID is configurable for every alert, which can lead users to a callback; Rave Alert also features an option to configure "Inbound calling" where users are connected to a number hosted on the Rave platform with very high capacity (3600 calls/minute) and that can be toll-free or as a local exchange which supports customized names on the Caller ID for those numbers. These lines may be used as a hotline and feature a one-click option to use these numbers as the Caller ID so that return calls route to your recorded message to keep 9-1-1 and other critical call centers from being overwhelmed by call recipients calling back for information.

		Yes	3rd Party	Next Release	No
2.16	The message initiator must have the ability to listen to the text to speech message before the message is initiated. Describe how the solution will meet this requirement.	Yes			

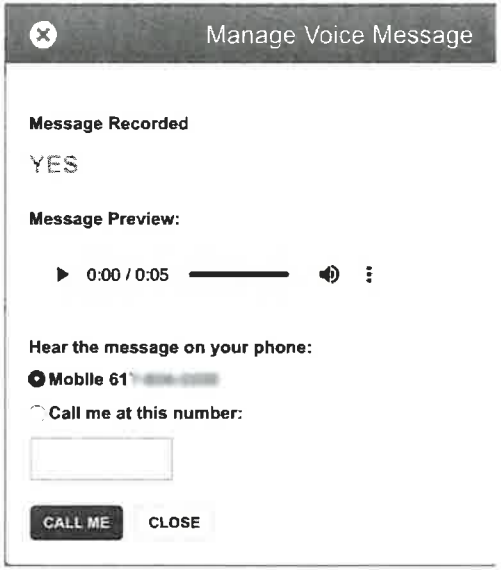
Bidder Response:

Compliant. Several options are available to audition both text-to-speech messages as well as recorded messages and our unique Introductory Voice feature that puts a user-friendly greeting as a prefix to your voice alert:

1. Within the Voice alert delivery mode, there is a play option to review the message at any time
2. When recording a message, you can preview within the Call Me function prompting the user to record the message - then listen and correct if needed.
3. The system can be asked to call a phone number to play the preview message.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

4. The user can dial in to the voice center to request a manual replay.



In general, the live preview within the Voice recording interface is the most commonly used.

		Yes	3rd Party	Next Release	No
2.17	The message initiator must have the ability to set the delivery speed/throttle rate for telephony type messages to be sent. Describe how the solution will meet this requirement.	Yes			

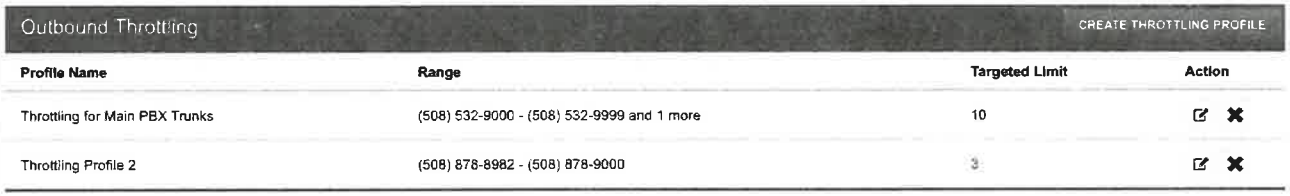
Bidder Response:

Compliant. Standard functionality. Rave Alert has both automatic and proactive call throttling tools to avoid and respond to congestion on your local telephone lines.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

During real-time delivery, Rave Alert uses congestion-based throttling to automatically avoid overwhelming local exchanges. For example, each of Rave Mobile Safety's 4 voice-calling centers' ARS (Automatic Route Selection) tools maintain at least six premier carrier route choices to deliver individual voice alerts.

These systems can change routes and carriers in real-time to bypass faults or congestion. Rave Alert also supports configurable throttling so you can tune our call output to your local constraints. You can identify both the phone numbers that should be throttled (in the form of line ranges) and your desired call rate. When sending messages, Rave Alert will automatically collect the phone numbers associated with a throttling profile, group them together, and begin calling these numbers, limiting calls to the maximum concurrent call limit set in the throttling profile.



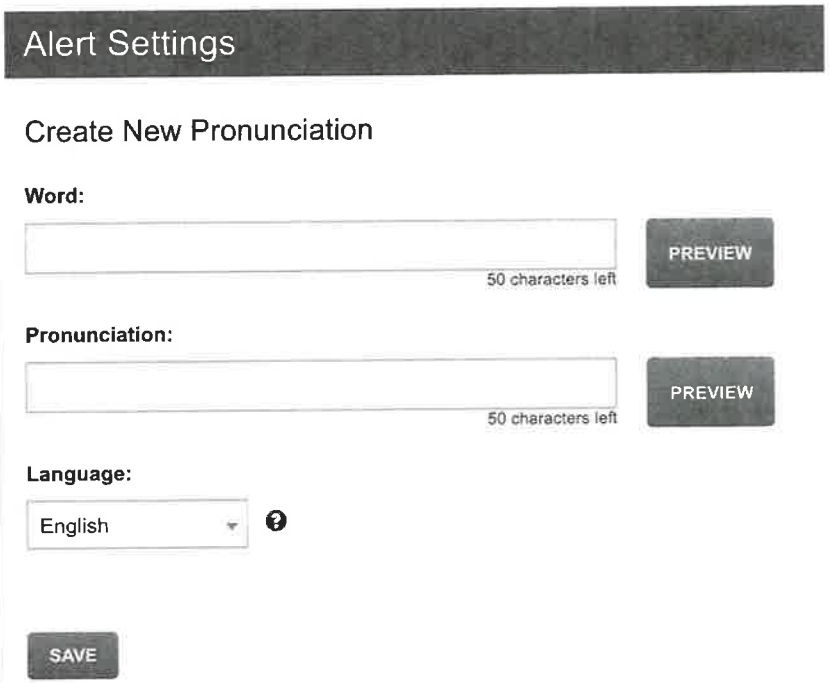
Rave Alert automatically determines the call rate based on the limit you define, the number of recipients, and the length of the call message to maximize throughput without overwhelming your infrastructure. You can create multiple throttling profiles for independent voice networks if needed. For instance, if you have a legacy PBX system and a newer VOIP system, each with dedicated capacity and distinct phone numbers, you can create corresponding Throttling Profiles to match each system's voice capacity.

		Yes	3rd Party	Next Release	No
2.18	The EMNS must have the ability to store special pronunciations in the system so that when a word is typed in an outgoing message the word is pronounced as phonetically stored in the system. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Standard functionality. System administrators can fine tune pronunciations directly within the System configuration interface:



		Yes	3rd Party	Next Release	No
2.19	The EMNS must have the ability to address the recipient by user name as a greeting at the beginning of the message as a default setting. Describe how the solution will meet this requirement.				No

Bidder Response:

At this time, Rave Alert does not support this functionality out of the box.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
2.20	The EMNS must have the ability to set default message sending methods by division or group. Example: a specific group could always default to: "round robin" method unless overridden at the time the message was initiated. Describe how the solution will meet this requirement.	Yes			
Bidder Response: Compliant. All template settings (given permissions) can modify all template alert settings as needed.					

		Yes	3rd Party	Next Release	No
2.21	The initiator of a message must have the ability to override device preferences. (Example: the administrator must have the option to call "work phones only" during a notification even though the primary device listed in a recipient preference is "mobile phone" the only device called for this recipient in this example would be "work phone") Describe how the solution will meet this requirement.	Yes			
Bidder Response: Compliant. Standard Functionality. Device types and placeholder columns are combined to select specific settings as configured. Some additional functionality is available based on specific feature areas; for example, Automated Weather Notification functionality and opt-ins can be configured to support specific whitelisted hours for each weather type if desired. Values presented to the activator will be specific to selected delivery modes for the alert; all choices are active based on alert settings.					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

Text
- (●) All Text Devices
- ( ) Select Text Devices

Email
- (●) All Mailboxes
- ( ) Select Mailboxes

Voice
- ( ) All Voice Devices
- (●) Select Voice Devices
  - [x] Mobile 1
  - [ ] Mobile 2
  - [ ] Mobile 3
  - [x] Land line 1
  - [ ] Land line 2
  - [ ] Land line 3

		Yes	3rd Party	Next Release	No
2.22	The EMNS must have the ability to include rich media attachments on email notifications. Bidder describe process. (add this type of sentence to all requirements.)	Yes			

Bidder Response:

Compliant. With Rave Alert you can customize the subject, content, Display Name (which displays as user name in email clients such as Outlook and Gmail), from:, and reply-to: addresses of each email alert, and the format of HTML emails, including embedding images, embedding links, and formatting reusable headers and footers. To make that process faster and prevent typos, you can save collections of address and format settings into quick-access profiles for your administrators to choose when sending alerts.

Rave Alert supports up to 10mb of attachments or up to 10 attached files to email alerts. You can save these attachments ahead of time as part of alert templates, or upload them at send-time as needed.

A key factor is that both image and file attachment content are stored on high-performance Rave servers. Email administrators appreciate the efficiency of this methodology, which minimizes the size of messages sent and stored on mail servers, and at the same time maintains optimal delivery performance.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
2.23	The message initiator must have the ability to control how call-outs must be terminated, including but not limited to: a. All recipients defined for notification have been reached; b. The pre-determined time period comes to an end; c. A selected number of unsuccessful attempts to reach a recipient has been reached; d. A pre-determined number of recipients from a larger list have been notified; e. Pre-determined positions have been filled by desired number of personnel; f. The callout is stopped manually. Describe how the solution will meet these requirements.	Yes			

Bidder Response:

The message initiator must have the ability to control how call-outs must be terminated, including but not limited to:

All recipients defined for notification have been reached;

Compliant.

The pre-determined time period comes to an end;

Compliant. Set via alert expiration.

A selected number of unsuccessful attempts to reach a recipient has been reached;

Compliant. Can be configured in modes such as voice based on number of attempts. Other retries are tied to alert expiration.

A pre-determined number of recipients from a larger list have been notified;

Compliant. Rave Alert notifies all users on selected lists. Several workflows can be used to sub-segment lists and subscriber populations.

Pre-determined positions have been filled by desired number of personnel;

Compliant. Quota functionality is standard within Rave's Polling Alert type.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

The callout is stopped manually.

Compliant.

Describe how the solution will meet these requirements.

Compliant. Rave Alert provides mode-specific stop and cancellation behaviors appropriate to the delivery mode, as well as the ability to cancel an in-progress notification.

First, every alert can be configured for a customized expiration period, defaulting to 8 hours.

Every active alert may be cancelled, shutting down all delivery and retry behaviors in the system, and executing mode-specific behaviors with additional modes such as IPAWS, CAP, and others. In addition, IPAWS, CAP, and Alertus notifications all support configurable expirations via standard settings, accessing mode-defined configurations.

In addition, specific requirements are met via other features. For some delivery modes, notably voice notifications, where retry behaviors may be configured for a certain number of retried calls over user-defined intervals.

Rave's location-aware Polling features also support settings to expire at the default alert expiration time, any arbitrary period ranging from 15 minutes to 60 days, and when a quota response is met - e.g., when 5 users have accepted an invitation, the next respondent is notified that the request has been satisfied.

A key component to understand all these behaviors is reporting: Rave Alert shows summary views indicating statuses mode-by-mode and alert-wide; detail reports will show the impact on every user and every device selected for notification.

		Yes	3rd Party	Next Release	No
2.24	The EMNS must be able to receive a response from two way devices to confirm a message has been delivered. Explain the methods.	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Alert supports individual responses from recipients for voice, text, and email alerts, both in standard alerts and via our polling notifications. Some of Rave's mobile apps support check-in response features as well.

We support phone polling using touch-tone responses. On voice notifications, the administrator can configure the notification to have up to 9 responses, and instructs recipients on the required responses when recording the message. Voice response collection can be configured in alert templates for instant recall. Responses can be required or not as desired.

Rave Alert also supports 2-way communication for text and email. For text notifications, Rave Alert supports inbound SMS responses. For email notifications, Rave Alert supports configurable, one-click accessible "email profiles" that can be attached to email alerts and alert templates. The profiles store combinations of "from:", "reply-to", and "Display Name" SMTP attributes that properly brand email in the user's email clients, and can selectively route responses to specific mailboxes.

Rave Alert generates a dedicated response report for every alert that records responses from any of these tools. Each incoming response generates a push notification to the alert sender with a link to this response report. Alert activators can receive a push notification when responses are received.

This, in addition to the previously mentioned and robust polling features ensure a two-way messaging process that can be trusted to deliver the appropriate feedback in an easy to manage fashion.

		Yes	3rd Party	Next Release	No
2.25	The EMNS must be able to receive polling information (Example: "press one for Available, press 2 for Deployed, or press 3 for Out of Service"). This ability must be available in some form for all two-way devices and a call back method must be available for one-way devices. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. As noted above, Rave Alert processes two-way responses from recipients for standard voice, text, and email alerts as well as its powerful polling features.

We support phone polling using touch-tone responses and text replies on individual delivery modes like SMS and email.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Rave Alert generates a dedicated response report for every alert that records responses from any of these tools. Each incoming response generates a push notification to the alert sender with a link to this response report.

One additional note is that Rave Alert's polling notification type does NOT require that the recipient have a mobile app installed; all functionality works on any Internet-connected device, such as desktops, laptops, smartphones, tablets, MDTs and more.

		Yes	3rd Party	Next Release	No
2.26	The EMNS must have the option of allowing the recipient to hear the message repeated. Describe how the solution will meet this requirement. (Example: "press zero to hear this message repeated")	Yes			

Bidder Response:

Compliant. Every voice alert supports a "Press * (star) to repeat" option to include or exclude as desired. In addition, on voice notifications, message replays can be configured to repeat the message up to 10 times.

		Yes	3rd Party	Next Release	No
2.27	There must be a feature that requires a PIN or other authorization of receiver for secure messages before delivery. (Example: "enter your PIN to listen to this message"). Describe how the solution will meet this requirement. If additional authorization criteria is available, please list:				No

Bidder Response:

There must be a feature that requires a PIN or other authorization of receiver for secure messages before delivery. (Example: "enter your PIN to listen to this message"). Describe how the solution will meet this requirement.

At present, Rave Alert does not support this function. It would require a product enhancement to provide. Rave Mobile Safety is interested in learning more about the underlying use cases for this function to explore potential enhancement paths to meeting this requirement in a future release.

If additional authorization criteria is available, please list:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

At present, Rave Alert does not support this function. It would require a product enhancement to provide. Rave Mobile Safety is interested in learning more about the underlying use cases for this function to explore potential enhancement paths to meeting this requirement in a future release.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

	Contact Management Requirements Section 3	Yes	3rd Party	Next Release	No
3.1	The EMNS database must be capable of allowing system administrators to add or delete contact numbers from the main database or any databases created by the same administrator at any time and provide an audit trail to search and inspect changes and deletions. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Extensive fully-auditable user management functions are supported, all observing administrative access permissions for the users who are managing contacts. Mobile, voice and email addresses support a "Test" button that can be used by an administrator to test connectivity if desired; these also appear to the end-user in self-service portals for self-testing. Rave's automated SmartLoader tools provide a platform for fully automated contact management functionality described in surrounding responses.

Certain other automated or pre-provisioned data can be managed. For example, ANI/ALI/911 loaded into the system by automation may have devices suspended permanently. In the use case where a former resident has ported a local phone to another locale, you'll be able to suspend that contact and it will stay suspended over multiple refreshes to the data.

Inside the product, a manual interface supports auditable manual account management, and there is a spreadsheet-based upload process that can be used to load multiple users quickly via a single action.

One feature set worth noting is that user management can support users who may need to manage user data ONLY, or who are assigned delegated user management tasks where access to user updates and affiliations are de-centralized.

		Yes	3rd Party	Next Release	No
3.2	The EMNS must have the ability to import contact information from any database via secure file transfer protocol. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert offers multiple tools to accept data from different databases.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

SmartLoader
Rave Alert offers a suite of batch-oriented data automation and ETL capabilities called SmartLoader. In Rave Alert's batch interface formats, a CSV file-based upload process supports a full contact upload as well as segmentation of users into messaging groups.

You can use SmartLoader to automatically:

- Add new users to Rave
- Opt users in to Broadcast Alerts via e-mail, text, and voice message depending on provided device contact information
- Remove members from Rave who do not appear within the batch file
- Update attributes such as phone and email contact information associated with existing users when re-running an updated batch file
- Create and manage groups and group properties
- Manage group subscriptions

SmartLoader can be configured to automatically update and sync data with other databases as personnel information changes.

Over 35 points of validation are supported by the SmartLoader utilities, including scanning for duplicate records. For example, Rave Alert validates both mobile carrier and whether a specific mobile number is in service. This implementation provides a "set it and forget it" style of ongoing management of subscriber data in and out of the ENS.

Transport can take place over public shared key SFTP or WebDAV connectivity if desired.

Managed Contacts
Rave Alert also supports broad functionality for manually loading contact information for guest or temporary users using our Managed Contacts feature.

Managed Contacts lets you create, edit, and delete user records by loading a CSV file, with the ability to specify start and expiration dates, multiple contact points per user, group affiliations, and geo-tagging and address data for contacts for use with geographically targeted notifications.

User Management API
The Rave User Management API allows for management of subscriber data, group properties, and much more, directly from within

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

bespoke applications such as portals and personnel systems. It is a robust user management API that can support real-time user management via SOAP-based or RESTful web services applications. Remote applications can create users and manage the system through this API. The API also supports all list and group functionality in the product, as well optional interactive services supporting a mobile phone confirmation flow. Manual management tools for help desk or other administrative users with assigned permission levels, are also available.

These APIs also support messaging to individual recipients by SMS and voice, allowing you to embed notification functions in response to application events. This feature is not designed for mass notification.

HR Systems and Other Databases

Rave Mobile Safety has experience integrating with a wide variety of HR systems and other databases using the tools described above. Update schedules are configured based on customer needs, with data refreshes performed anywhere from daily to yearly.

Ongoing Data Validation

Once data is entered into the system, Rave Alert continues to automatically check its validity through periodic "freshness checks." The outcome of these are captured in a standard Enrollment Report, a daily report that includes all customer-stored internal user data in the system, all user preferences, and any validation issues that emerge from freshness checks. This report is an automated nightly snapshot stored for 30 days in rotation for the customer. The customer can archive these reports locally manually or via automation to create a complete historical record of such data if desired.

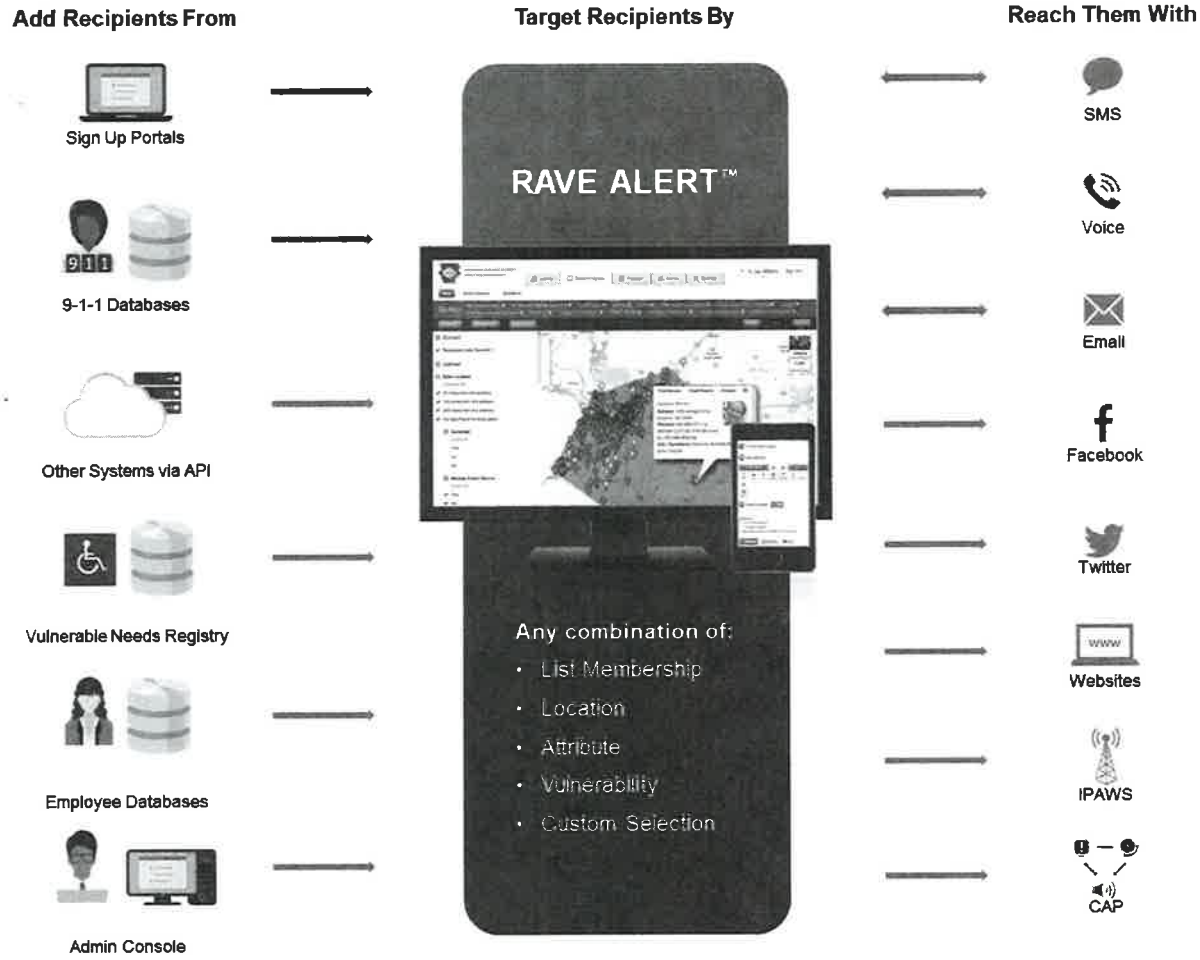
		Yes	3rd Party	Next Release	No
3.3	The EMNS must offer (as an option to divisions that require the additional service) a solution that must automatically synchronize the division's contact list with the system database. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert supports many ways to migrate or upload contact data and recipient lists, including the ability to upload an ad hoc list at the time of message activation. We support unlimited user lists, unlimited recipients per list, and unlimited recipient

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

lists per alert. Our Optional Smartloader solution allows for synchronization of data from external systems into the Rave Alert platform.



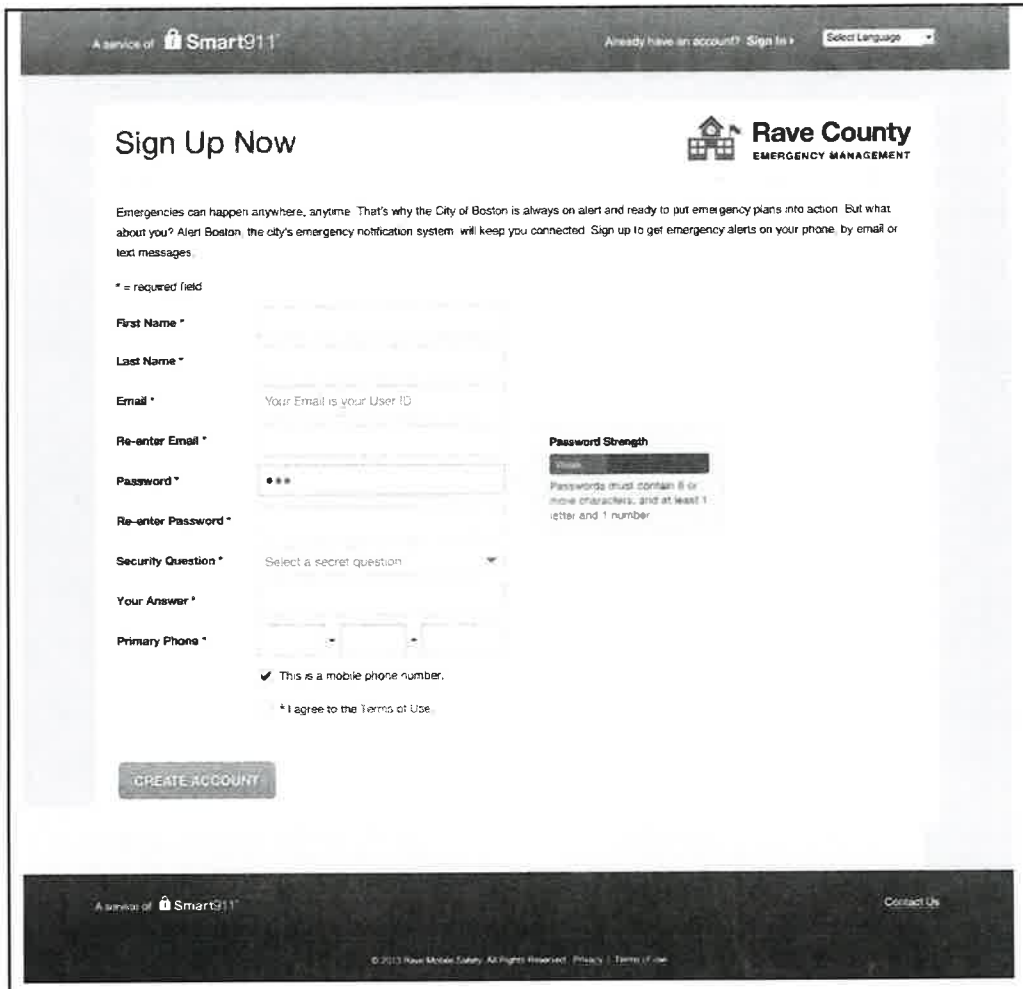
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
3.4	The EMNS database must be able to store unlimited devices per database contact and should allow a different calling order of these devices depending on the time of day (location schedule). (Example: recipient might designate a work phone as the primary device between 0700 and 1800hrs, a home phone as primary device between 1800 and 2400hrs.) Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert provides a public portal where residents, commuters, and businesses can add and update contact information. Links to this portal can be embedded directly into client websites. This portal is a standard part of our alerting services, and has no additional cost or setup fee.

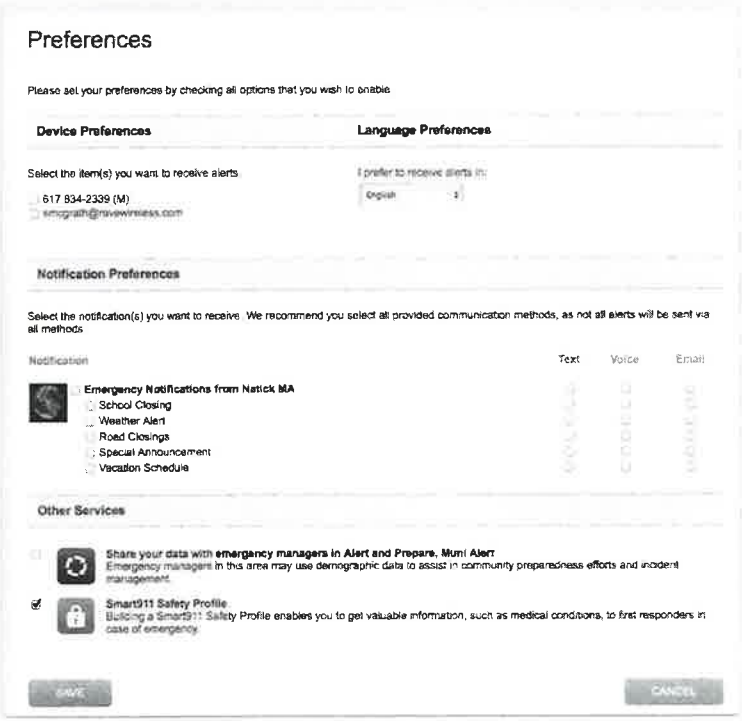
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



This portal can offer different alert categories based on the registrant's location, allowing you to intelligently support both resident and commuter populations. Community members can input unlimited contact numbers, including wireless devices. Information that your community members put on this portal is updated in real-time on the system and available for use immediately.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

You can configure different opt-in subgroups for your users to choose from, shown in the "Notification Preferences" section below. Users can choose what type of alerts to receive, and what devices to receive them on, with a selection available for each device selected for contact:



Keeping data current is always a challenge when providing citizen services to the public. Our public portal does this for you with a sophisticated automated reminder system, which requires your recipients to verify and update their data every six months. This keeps your alerting lists and vulnerable needs registries accurate and up-to-date.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

The public portal also provides unified sign-up and opt-ins for our other safety products in the Rave 911 Suite, allowing your users to share emergency data with 9-1-1 and personal vulnerabilities with emergency managers while signing up for alerts. Jurisdictions using both Rave Alert and the Rave 911 Suite report higher registrations for both services thanks to this unified signup.

As noted in other responses in this bid, Rave Alert supports a separate portal for staff and employees, conveniently isolating staff updates from public updates in order to best support the unique communications needs unique to your jurisdictions and agencies compared to strict public communications. Our Staff portal may implement device management such that particular contact container fields can be used to signify opted-in personal device contact fields from official devices, office phones, etc. Within alerting workflows, sends have options to target these based on the type of device indicated when needed.

Other specific features also support related features. For example, Automated Weather Notifications can specify notification hours customized for each severe weather type if needed. All Common Alerting Protocol integrations support time-of-day filters for notifications as well.

		Yes	3rd Party	Next Release	No
3.5	The EMNS must allow for each political subdivision and its separate departments or entities to open unlimited sub-accounts with their own secure password and identification. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. We offer UNLIMITED admins with customizable permission levels so you can adjust and assign access to different Rave Alert tools in ways that match your current organizational structures and emergency management procedures.

Rave Alert supports standard roles with defined and distributed permissions, and you can create **custom roles** to configure access to nearly every product feature and every delivery mode in your system. You can stipulate, for example, administrators' read-only or read-write access to subscriber data, their ability to create or edit groups, save templates, manage alert distribution lists, and much more. The interface will only show your administrators tools they can use, simplifying the system for people who need to quickly send alerts without distractions, and supporting distributed administration models within your organization. This enhances both ease of use and organizational security.

Custom roles can also control access to specific data objects within the system, for example:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

- Selective access to recipient groups (with or without create and save permissions)
- Selective access to individual alert templates (with or without create and save permissions)
- Selective access to delivery modes such as text, voice, email, and social media, as well as integrated systems such as sirens, IPAWS, and digital signage
- Selective access to specific social network pages or accounts on Facebook or Twitter
- Selective access to website feeds, e.g., where administrators at one location should only publish to specific websites
- Selective access to profiles that function as presets for *branding and administrative settings* such as Caller IDs on voice calls and email header and footer content
- Selective access to the Shape Library shapes available in the system
- Selective access to reporting features
- Selective access to a range of tools for managing subscriber data
- Selective access to Rave Prepare functions supporting emergency management decision making
- Selective access to system administration and related configuration settings
- Selective access to multiple IPAWS COG profiles

When an administrator/activator is assigned an RBAC role, the user is instantly assigned feature permissions, specific objects such as templates, subscriber lists, accounts and profiles, all from a single assignment. These powerful tools make for a safer system that removes functionality not appropriate to users in roles and at the same time simplifies activations by showing only relevant features.

		Yes	3rd Party	Next Release	No
3.6	Division administrators must have the ability to control access to each of their databases or to subsets of data within their databases. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Please see previous response. When an administrator/activator is assigned an RBAC role, the user is instantly assigned feature permissions, specific objects such as templates, subscriber lists, accounts and profiles, all from a single assignment. These powerful tools make for a safer system that removes functionality not appropriate to users in roles and at the same time simplifies activations by showing only relevant features.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

We support customizable permissions that allow you to delegate read- and/or write-access to specific groups of people, so specific administrators can alert the specific groups of users they need to. Administrative "scope" can also be managed, offering different levels of administrative assignments even among peers within a department of sub-organization. For some customers, a "Read-only" view option has been useful for Help Desk staff supporting internal users; such users can manage people with NO access to alerting features if desired.

		Yes	3rd Party	Next Release	No
3.7	The EMNS must be capable of storing: a. An unlimited number of call recipients; b. Data for each recipient in unlimited number of notification groups or lists; c. Updates or changes to recipient information and have those changes reflected in repeated records for every notification group where the recipient is listed. Describe how the solution will meet these requirements.	Yes			

Bidder Response:

An unlimited number of call recipients;

Compliant.

Data for each recipient in unlimited number of notification groups or lists;

Compliant.

Updates or changes to recipient information and have those changes reflected in repeated records for every notification group where the recipient is listed.

Compliant.

Describe how the solution will meet these requirements.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Alert does not limit recipients, contact data, list affiliations, or other data. Note that the system minimizes duplicate contact issues in two ways: on the data side, our advanced database tools enforce database best practices when possible for intelligent data management across our services; on the more important notification side, when you send alert, Rave Alert de-duplicates your alert to the individual contact level - each selected device receives only 1 message. To reach all critical message recipients, simply include the right user lists and let the service manage all duplicate devices.

Rave Mobile Safety was founded in 2004, and has been providing high performance, high-reliability mass notification services, built from day one on a robust, geo-redundant hosted platform - for over 15 years. Rave's safety systems currently support far in excess of 55 million users, and Rave's products are used throughout the US, in hundreds of 9-1-1 Public Safety Answering Points PSAPs around the country and are built on a substantial platform architected for scalability and growth while maintaining the highest levels of security and reliability. Details are provided throughout this response.

Rave's products are used in large cities such as the City of Seattle WA since January 2015, and in many other numerous large cities, towns, and counties across the United States. Overall, Rave technically is used in over 3,100 communities across all 50 states. Seattle uses Rave Alert for public notifications as "AlertSeattle" including over 600,000 landline devices from ANI/ALI data, as well as for numerous departmental and operational notifications, including large police and fire operations staff and the Office of Emergency Management. The Seattle Center, the city's central hub for museums, recreations, a stadium, and buildings that house 4,000 city employees and many affiliated contractors such as food service workers and security; after a violent incident in a food court, their Rave system was configured to support a public opt-in as well as access to city HR information for impacted employees across several city departments. In addition, the Seattle Public Utility supports urgent notifications, which is implemented to support both geographies within city boundaries, but also some additional extensions where the City utilities provide services to surrounding jurisdictions.

Rave has performed substantial statewide implementations of multiple products in the States of Arkansas, Delaware, Michigan , Louisiana, Oklahoma, and the District of Columbia, and in similar large regional deployments around the US. Our systems provide coverage to large customers where multiple customers overlap regional. Over 26% of all emergency calls to 9-1-1 delivery key data through Rave's systems.

Rave's systems sent over 2 billion messages in 2019, and our platform has been built for scalability, capacity and growth.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
3.8	Administrators must have access to and be able to modify all user profiles. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant via several components and workflows including: Export functions are available in several report formats depending on data source. Specific data exporting and create/edit/delete functions may vary depending on intake point (portal, manual add, ad hoc load, staff record, etc.) and may vary based on type of user record. Tools range from automated data reports available in secure storage environments, one-click export features available to permissioned administrators, guided support for those assisting citizens with subscriptions, and data management/ETL tools supporting IT functions and *ad hoc* user account provisioning within product user interfaces.

Permissioned users are provided with an editor to create, search, edit, suspend, assign to roles, or delete users. This view of the system can be supported without access to alerting features if desired (for example, for help desk staff who should not be permissioned to send notifications). All access to data management tools in Rave Alert are access controlled to provide secure access to data. Rave supports both user-initiated and admin-initiated test messages and other validations when working with subscriber contacts.

Subscriber Database Creation
Rave Alert's data model focuses on contact data integrating sources from internal staff data, citizen opt-in information with household information, and all the data currently supported via Smart911 and 9-1-1/ANI/ALI database contacts from a variety of potential sources in jurisdictions where it is available, geo-targeted addressing via citizen-provided, sanitized data (i.e., with address corrections and geographic adjustments optionally provided by the citizen), and IPAWs. Jurisdictions can create and manage accounts on behalf of citizens using our assistant tools on the public portals among other options; these features are often very useful when supporting public events encouraging residents to sign up for the service.

Updating the Database
Data records can be managed in product user interfaces or programmatically, or in combinations of both methods. In some cases, editing options vary by type of data. For example, for 911 address-based records loaded via automated processing, a persistent "Suspend" option is available for subscribers who opt-out but may reappear when provisioned 911 data sources are updated in the future - forestalling a subscriber privacy objection were a user re-enabled in the system against the directive of a previous opt-out.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

For staff data, all records are fully editable. Rave Alert provides multiple ways to edit and update the subscriber database. Through Rave Alert's batch interface process, a CSV file format represents your ERP, HR system or other database interface fields within a simplified structure. These data formats allow clients to:

- Add users to Rave who are not currently members of Rave
- Opt users into the receipt of Broadcast Alerts via e-mail, text, and voice message depending on the contact information provided
- Remove members from Rave who do not appear within the files
- Update attributes such as phone and email contact information associated with existing users when re-running an updated batch file
- Create and manage Groups and group properties
- Manage Group subscriptions

Rave Alert also supports a web-services API for User Management that allows secure, remote management of subscriber data programmatically. This API is complementary to Rave's automated bulk processing, and allows the user to manipulate subscriber information in the system. The API can perform all the available actions via bulk upload can be performed through the API. This API supports REST-based web services.

Rave Alert supports unlimited administrators in all available administrative roles at no additional charge. Rave also notes that a release of enhanced editing features is on our 2020 roadmap and noted in this response as tied to our next major release. This enhancement set addresses and optimizes the user experience (UX) to address specific use cases requested by customers, essentially extending functionality currently available in our public portals to support assisted account management and contact details. We believe current functionality meets practical account management very well; these enhancements will extend current behaviors further to optimize administrator workflows when managing public user accounts.

		Yes	3rd Party	Next Release	No
3.9	EMNS must allow administrators to add, update, and delete recipients individually or through an online import process quickly and easily. Describe how the solution will meet this requirement.	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Alert supports broad functionality for manually loading contact information for users. You can create, edit, and delete user records by loading a spreadsheet file, with the ability to specify start and expiration dates, multiple contact points per user, group affiliations, and geo-tagging and address data for contacts for use with geographically targeted notifications. You can also perform all the same actions directly within the access-controlled "People and Lists" user interface.

		Yes	3rd Party	Next Release	No
3.10	Recipients must have the ability to login to the service in order to update device information if administrator assigns these permissions. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave supports independent portals for internal State and jurisdictional staff and employees and for residents and citizens via our public portal and mobile recipient application. Users can be pointed at the appropriate portal to update records via standard account management.

Note that "internal" portals can optionally be tied to the State's enterprise authentication services, taking advantage of identity management platforms such as AD/ADFS/Azure and technologies such as SAML2, to provide single sign-on (SSO) convenience to your staff.

The internal portal allows any standard or automated contacts to be set to editable or read-only for the end-user staff member and can display both internal as well as public opt-in categories. Opt-in groups for either public or private portal self-service can be configured in a minute or two within the administrative interface.

		Yes	3rd Party	Next Release	No
3.11	Administrators must have the option to give recipients the ability to opt in or out of receiving notifications. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Alert provides a public portal where residents, commuters, and businesses can add and update contact information. Links to this portal can be embedded directly into client websites. This portal is a standard part of our alerting services, and has no additional cost or setup fee.

This portal can offer different alert categories based on the registrant's location, allowing you to intelligently support both resident and commuter populations. Community members can input unlimited contact numbers, including wireless devices. Information that your community members put on this portal is updated in real-time on the system and available for use immediately.

You can configure different opt-in subgroups for your users to choose from, shown in the "Notification Preferences" section below. Users can choose what type of alerts to receive, and what devices to receive them on.

Our **SMS Opt-In option** also supports additional ways to allow either public or internal staff users to opt-in to notifications and notification groups simply by texting a keyword to the service. These may be persistent opt-ins or customized by duration of days or up to a specific date. Not only does this reduce the friction of portal navigation and signup for the long term or focused on specific events - conferences, visits, county fairs, public gatherings of all kinds. This feature supports a fully customized Welcome message as well as Expiration message informing the subscriber of the expiration. SMS commands can also be used to opt out of

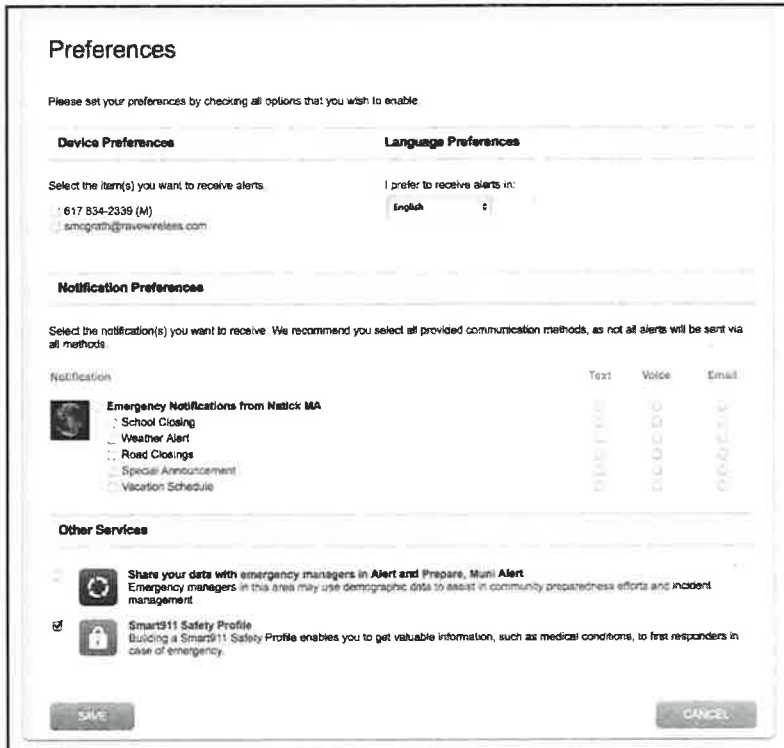
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

the system at any time. SMS Opt-ins may be *public,* meaning that anyone with the keyword can subscribe, or *private*, meaning only your staff members will be able to affiliate with these groups.

After opting-in to any choice by any method, the end-user is added to a recipient list that, when selected, chooses those devices and users for notification.

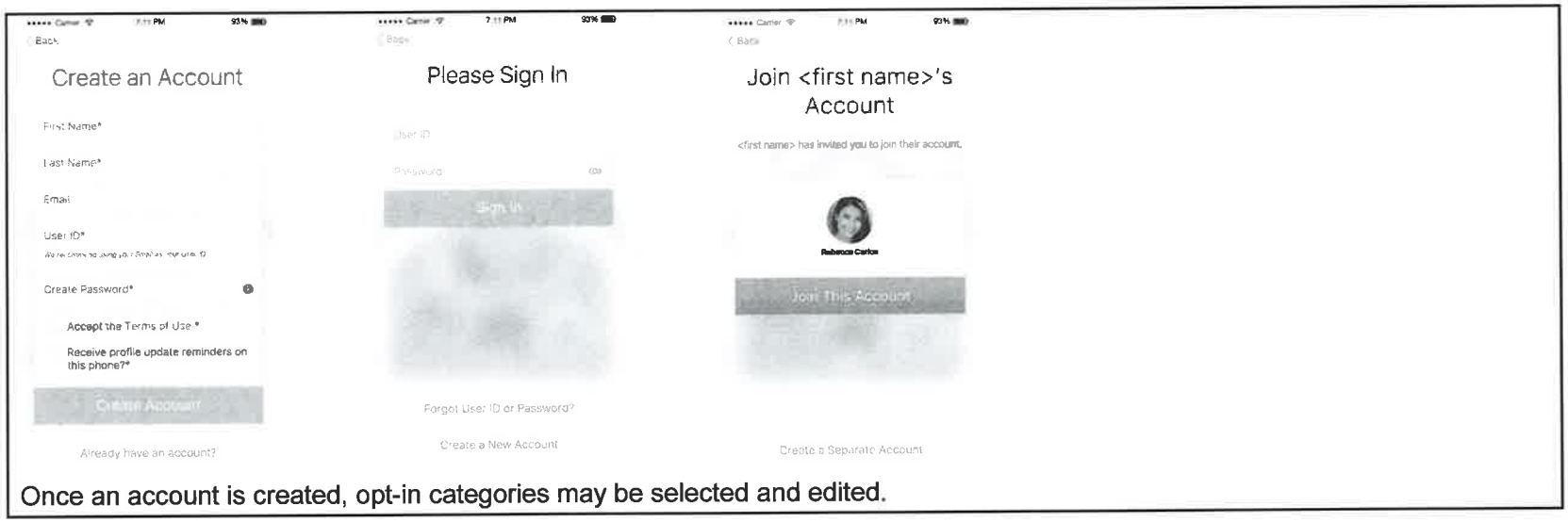
SMS Opt-ins, along with those managed on self-service portals, are interoperable. For staff or citizens who view their preferences on a portal, they will see "checked" boxes for any SMS opt-ins they've performed.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Users can perform all actions performed on the public portal directly within Rave's mobile apps. In the mobile app, the full account sign up process is available, as is the ability to join or leave opt-in groups.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Once an account is created, opt-in categories may be selected and edited.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Keeping data current is always a challenge when providing citizen services to the public. Our public portal does this for you with a sophisticated automated reminder system, which requires your recipients to verify and update their data every six months. This keeps your alerting lists and vulnerable needs registries accurate and up-to-date.

The public portal also provides unified sign-up and opt-ins for our other safety products in the Rave 911 Suite, allowing your users to share emergency data with 9-1-1 and personal vulnerabilities with emergency managers while signing up for alerts. Jurisdictions using both Rave Alert and the Rave 911 Suite report higher registrations for both services thanks to this unified signup.

Similar functionality is supported on our internal staff portal.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
3.12	The EMNS must allow for editing of groups, subgroups and management levels to be unlimited. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Customers are free to create and manage any number of groups in any combination without restrictions.

		Yes	3rd Party	Next Release	No
3.13	Layers and types of security must be provided for all user functions (one user may be allowed to perform all functions while others may be limited to performing restricted functions such as roster updates.) Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Robust details are provided in Response 3.5 above. Rave Alert's detailed RBAC permissions system ensures that users see only the content and templates, recipient groups, functionality, delivery modes, branding, profiles, IPAWS certificates, social media accounts and other features - that are correct for each activator. As noted in nearby responses, our RBAC controls support a delegated administration model to de-centralize management of functional and operational communications use cases such as this one.

		Yes	3rd Party	Next Release	No
3.14	All State of Nebraska data base information must remain in the continental United States even for redundancy or backup purposes. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. All State of Nebraska data, as with all our customers in the US and US government agencies, will be managed within the United States, including system data, all redundant datacenter locations where data may be mirrored or stored in clustered database infrastructure, and all encrypted backups.

	Yes	3rd Party	Next Release	No

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

3.15	EMNS provider must have an internet based self-registration page or provide a link from an agencies specified website to same type of page. Self-registration site must have ability to enroll and register their enrollment date, name, address, at least three cell phone numbers per enrollee, cell phone of highest priority and selection from a predefined list of at least ten notification event types. All Enrollment information data fields must be searchable and sortable. User name and password can be synced with existing databases such as Active Directory. System enrollment webpage must include agreement language, acknowledgment of use, explanation of system use, limitations of system and enrollee requirements. Also allows users to un-enroll voluntarily at any time. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. As noted, Rave Alert supports branded portals for both an internal employee/staff notification self-service option, as well as a feature-rich, highly accessible public resident sign-up process - initiated from the web or via our mobile app -- supporting multiple languages, support for assistants and residents who do not have email addresses, unlimited contact points and multiple users in a household, optional opt-in to provide critical information to emergency management - all with data validations and address and rooftop location adjustments for end-user addresses if desired. Citizens can follow a link to your branded portal; once they have created an account, any business or residence entered within a jurisdiction in the State that is using Rave Alert will be offered an opportunity to opt-in for its notifications.

Authentication and SSO integrations are available as options for internal and staff accounts to support your internal directory services and identity management platforms. All requested agreements, terms and conditions, and privacy policies as mentioned in this bid question are available on the portals and mobile app support websites. Rave's Community Marketing team also provides sample FAQ that can be hosted on jurisdiction websites describing your notification programs and registration links.

Note that Rave uniquely provides end-user subscription and account support, relieving your jurisdictions from the need to support routine account management issues, saving money and resources.

Further details about specific portal features follows:

Citizen Portal Overview

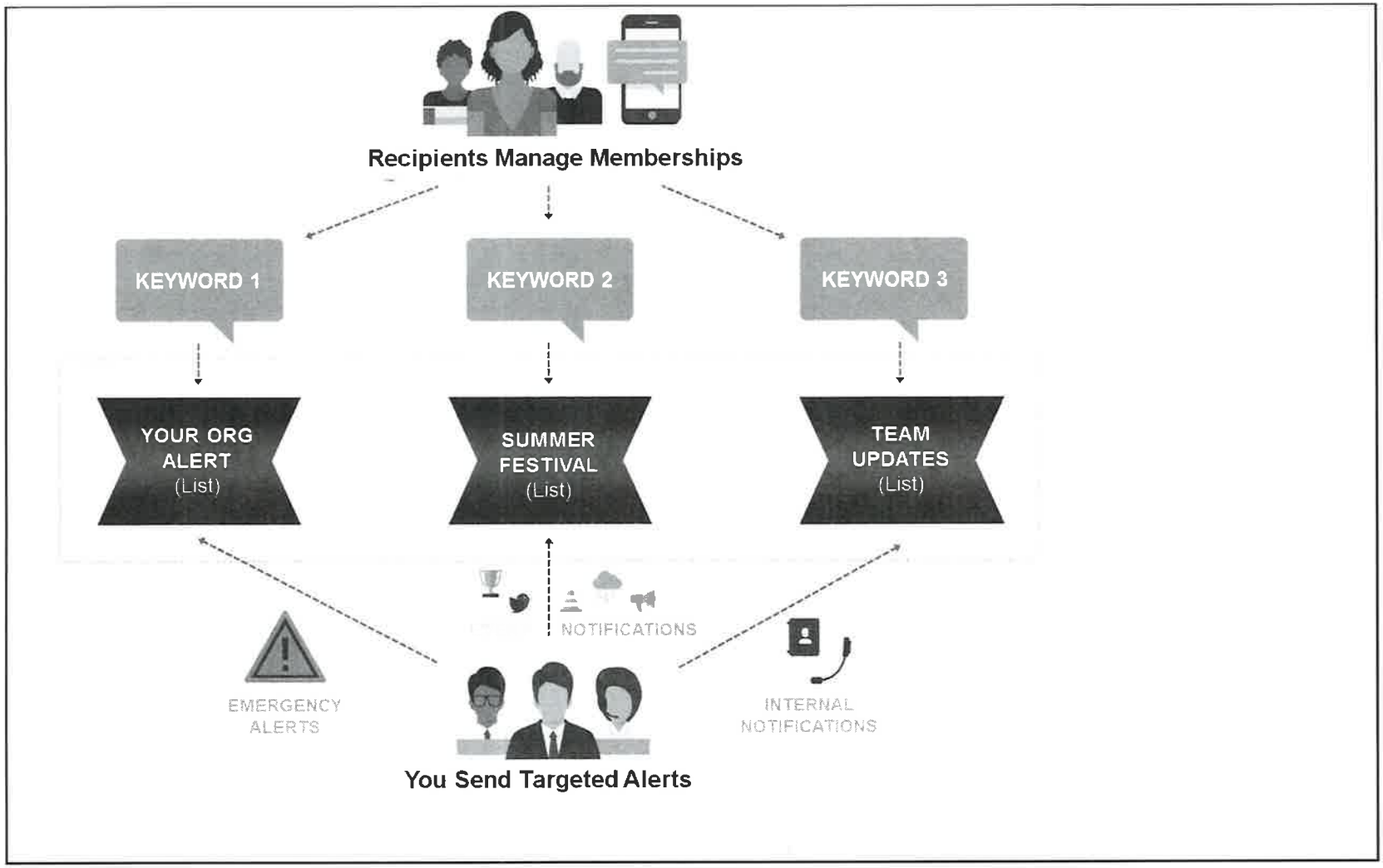
Citizens can always register on our web portal with a mobile phone number, a landline phone number, or an email address. They only need one contact point to register, and can perform all account functions, such as receiving account reminders and recovering

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

account credentials, through any contact point. This feature can be used in concert with our optional SMS Opt-in add-on to provide more ways for accessible participation in your notification programs.

Rave Alert supports an optional SMS Opt-in add on which lets your recipients subscribe to text alerts with just an SMS message. simply by texting a specific keyword to one of our shortcodes. This feature can automatically create text-only accounts for new users, no web-registration necessary. It can also provide an easy way for registered users to control their alerting preferences right from their phones, helping you meet recipient consent compliance rules.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

SMS Opt-in for Rave Alert allows a user to register for public or internal alerts by texting a keyword to a Rave shortcode. You can configure this feature to either allow new registrations or to validate numbers against your current database and only allow registered users to opt-in to alerts.

You can create custom welcome messages for these SMS registrants and, if desired, set registrations to expire after a certain pre-determined time, such as the duration of an event. And don't worry, this feature works seamlessly with our online portal - your recipients with accounts can opt-in through SMS or through their registered accounts and these settings will persist across both modes.

As an example use case, SMS Opt-in streamlines short-term notifications for large public events - fairs, voting events, and other large public gatherings. SMS messages are easy and quick, and keywords are easy to advertise. And instead of expecting recipients to unsubscribe manually, you can set registrations to only last within a specific date ranges. After each event concludes, you can update the keyword and re-use it for the next one, knowing no previous attendee will receive unsolicited new messages. SMS Opt-in is a Premium Module for Rave Alert and has an additional cost. Please see our pricing proposal for more information.

A common issue encountered in public notification subscriptions is supporting community members who do not have email accounts or rely on assistance from others to register for notifications. Rave's public portal platform provides specialized support for your communities facing these issues.

The portal enables email-less registration that allows citizens to register using alternative contacts, like phone numbers. This feature set improves program inclusiveness by removing a substantial barrier to entry for public notifications. It supports three critical capabilities:

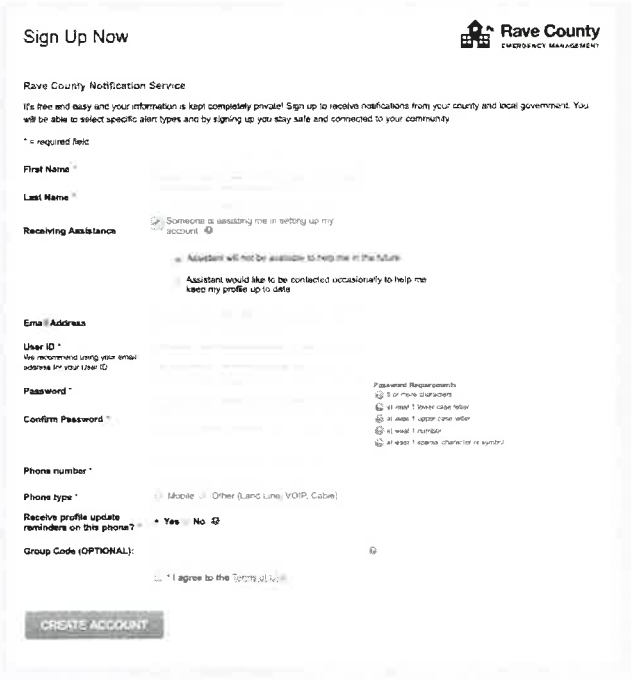
- Allows citizens to create an account using a phone number, where they can sign up for notifications, provide vulnerability data, and manage preferences
- Allows citizens to provide contact information of an " Assistant " who can help them sign up the Alert services, keep account information up to date, and receive account maintenance communications
- Allows citizens to recover forgotten account credentials without requiring an email address

Confirmations are customizable. Several validations can be enabled.

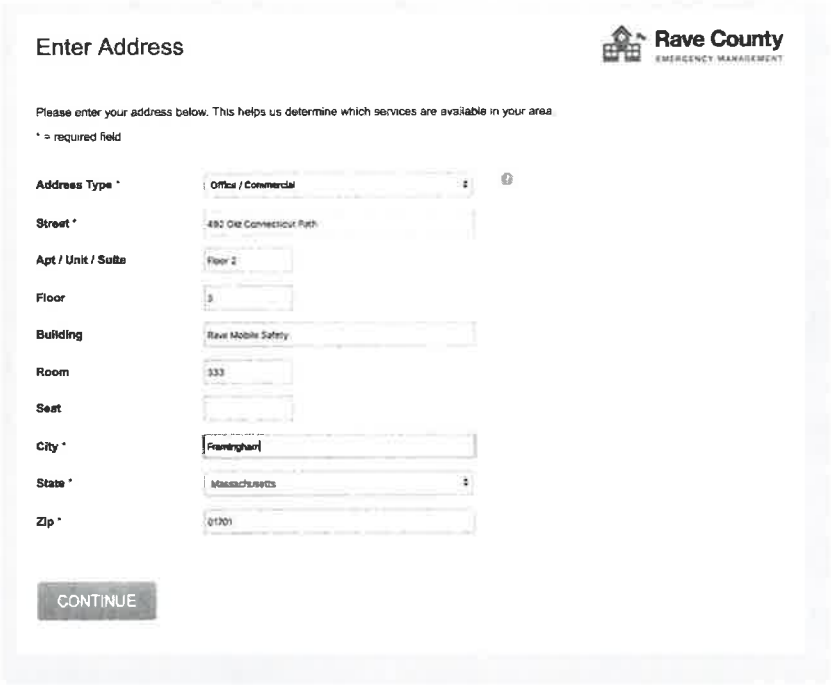
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Portal users are stepped through carrier validation and then are sent a short 6-digit code to confirm that the device is in the hand of the user. Our ERP integration also supports a function that will enable a feature to generate a fully custom "Welcome Email" that can offer content with links to resources for staff subscribers, a number of variable values, and any additional information of interest, sent the first time a new user is introduced to the system.

The public portal is a full self-service environment and has additional confirmation and capabilities. One feature often requested is the ability to support an Assistant or caregiver to manage someone's account, for example for residents of facilities such as nursing homes. Email is NOT required for registration, which diversifies the sign-up for members of the public without access to computers or email.

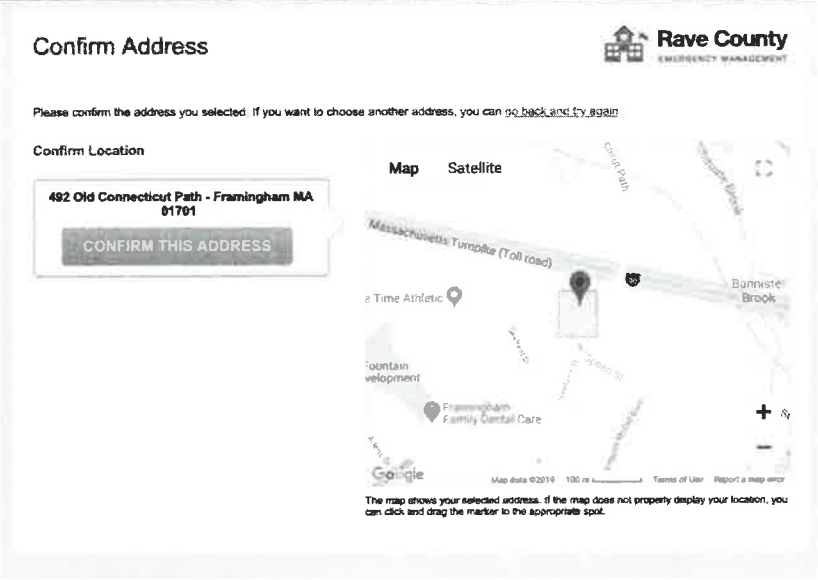


AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business



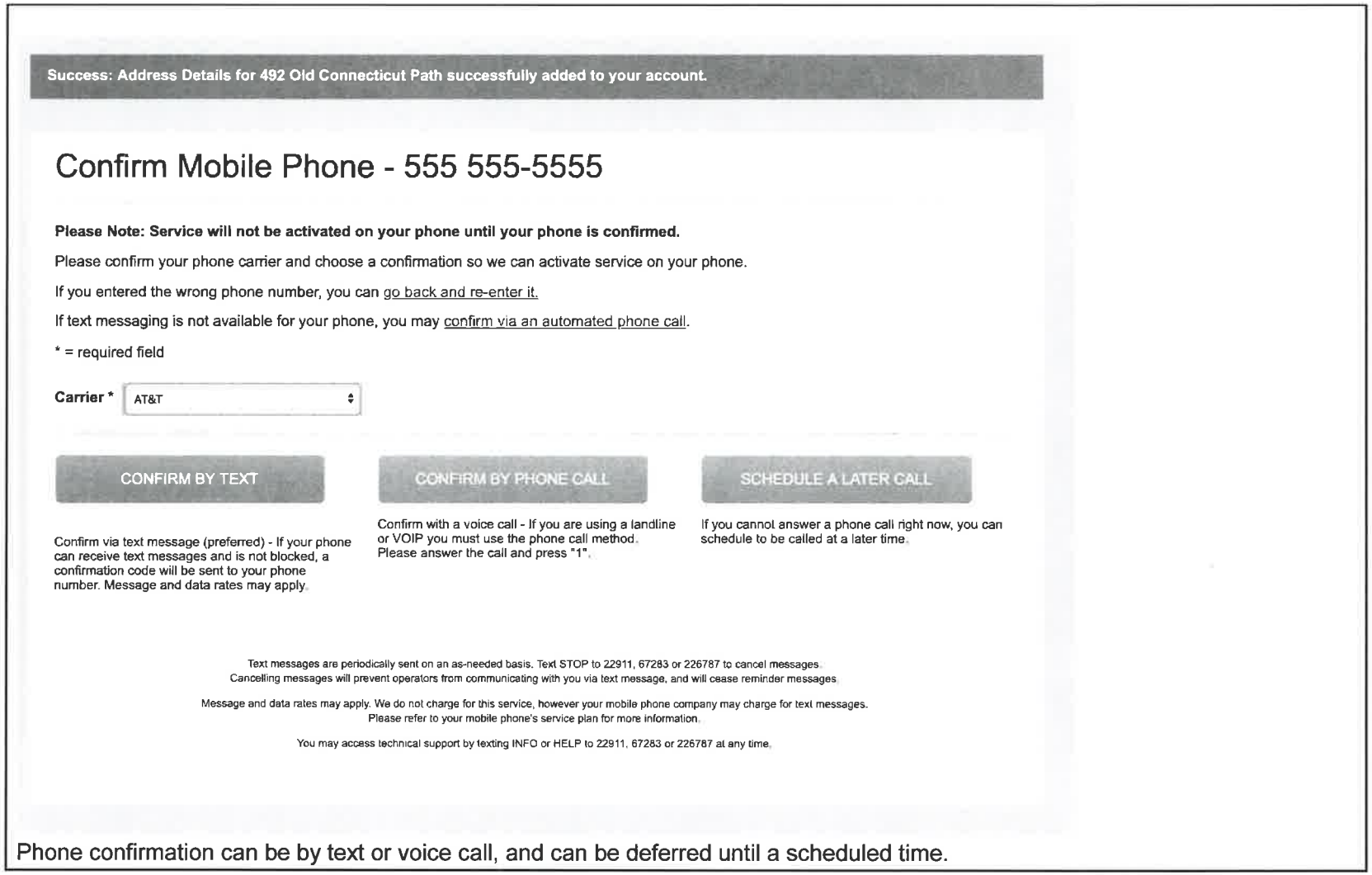
Address collection can be enabled or disabled for each referral.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



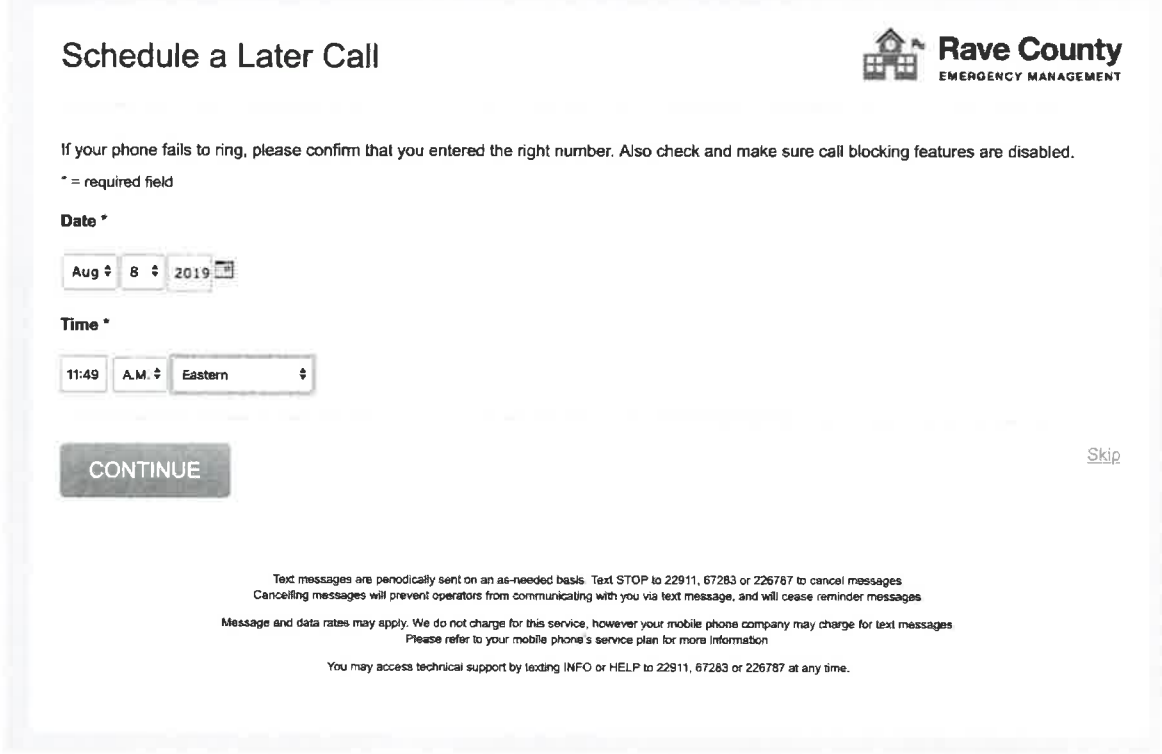
Addresses are shown in "cleaned-up" versions and the user can adjust the rooftop pin on the map when they see an inaccuracy. This keeps data clean when entering the system.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



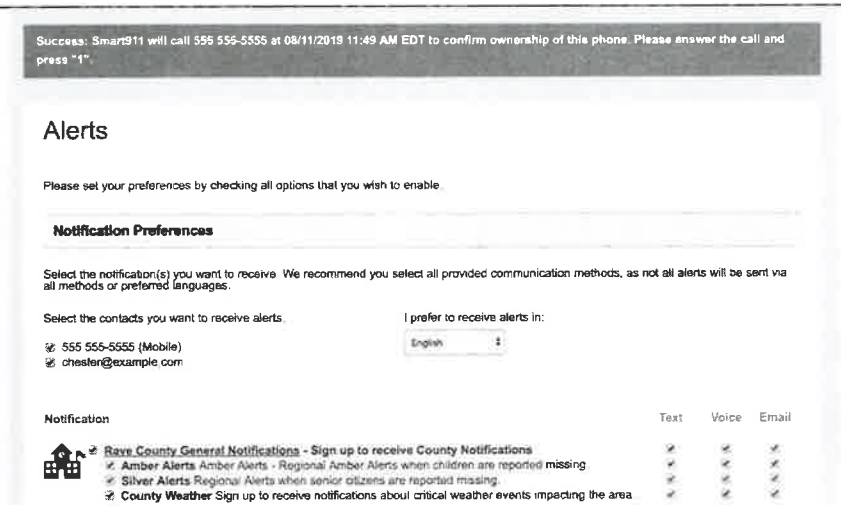
Phone confirmation can be by text or voice call, and can be deferred until a scheduled time.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Once confirmed, the user selects alert categories.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



In our mobile app, the experience is optimized for the smaller screen. A few examples:

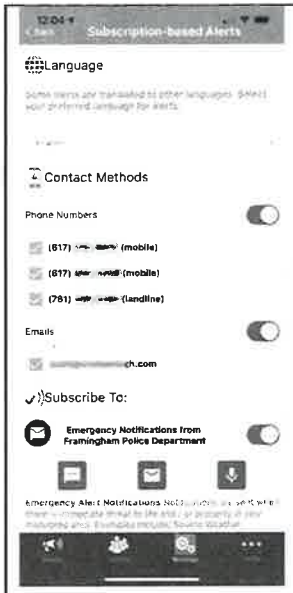
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Explanatory content displays an overview upon arrival. Account creation and contact validation can be fully managed within the mobile app as well as on the web.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Mobile phones are sent a confirmation code to complete device registration. When an account includes multiple contacts, the user may select those best to be used for notifications.

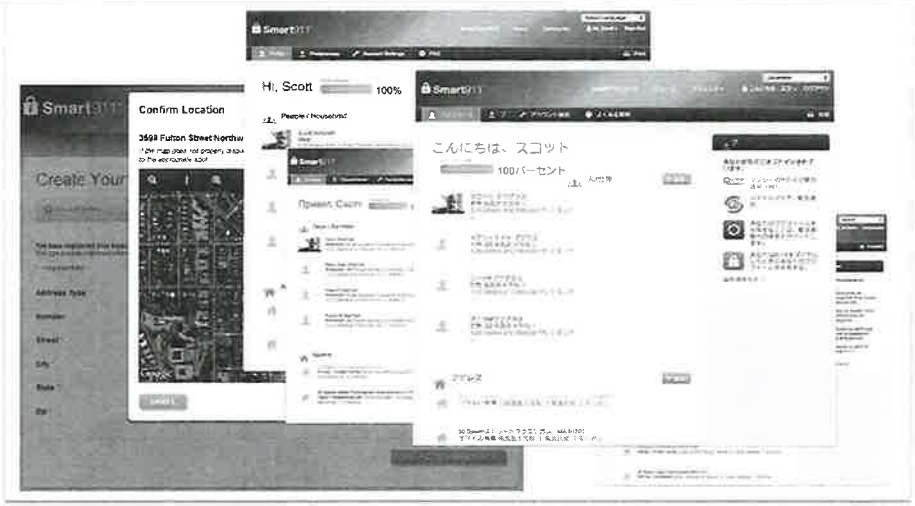
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Once contacts are enabled, the user can then manage language preference as well as subscriptions, selecting Text, Email and Voice delivery individually for each alert category.

Rave Alert's opt-in website where your community members subscribe and opt-in to receive alerts is fully translated in over 95 languages - including all instructions and content, with form descriptors.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Available Languages for System Website: All opt-in instructions and content can be translated into the following languages:

Afrikaans	Hindi	Polish
Albanian	Hmong	Portuguese
Amharic	Hungarian	Punjabi
Arabic	Icelandic	Romanian
Armenian	Igbo	Russian
Azerbaijani	Indonesian	Samoan
Basque	Irish	Scots Gaelic
Belarusian	Italian	Serbian
Bengali	Japanese	Sesotho
Bosnian	Javanese	Shona
Bulgarian	Kannada	Sindhi
Catalan	Kazakh	Sinhala
Cebuano	Khmer	Slovak
Chichewa	Korean	Slovenian

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

Chinese (Simplified)	Kurdish	Somali
Chinese(Traditional)	(Kurmanji)	Spanish
Corsican	Kyrgyz	Sundanese
Croatian	Lao	Swahili
Czech	Latin	Swedish
Danish	Latvian	Tajik
Dutch	Lithuanian	Tamil
Esperanto	Luxembourgish	Telugu
Estonian	Macedonian	Thai
Filipino	Malagasy	Turkish
Finnish	Malay	Ukrainian
French	Malayalam	Urdu
Frisian	Maltese	Uzbek
Galician	Maori	Vietnamese
Georgian	Marathi	Welsh
German	Mongolian	Xhosa
Greek	Myanmar	Yiddish
Gujarati	(Burmese)	Yoruba
Haitian	Nepali	Zulu
Creole	Norwegian	
Hausa	Pashto	
Hawaiian	Persian	

For outbound messages, Rave Alert supports optional multi-lingual messaging in text modes with automated translation via Microsoft-powered API integration, with up to 60 languages supported. This option is available to customers at no extra cost. In the alert template, the administrator enters English text, and can then click on the enabled languages to automatically translate the message text. Rave recommends machine-translated text be validated by a native speaker of each language; edited translations are stored in Rave's alert templates.

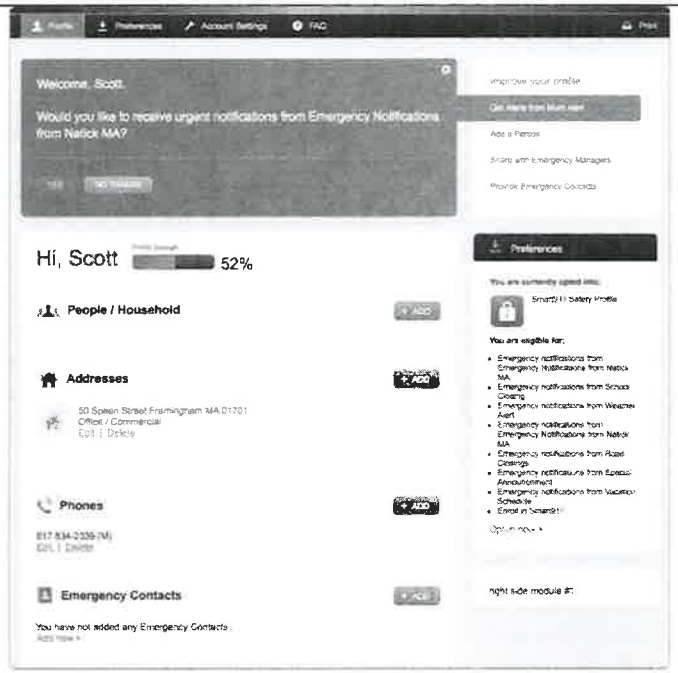
Automated translation of outgoing alerts are in the following languages:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Arabic	Hebrew	Queretaro
Bosnian	Hindi	Otomi
Latin	Hmong Daw	Romanian
Bulgarian	Hungarian	Russian
Catalan	Indonesian	Serbian (Cyrillic)
Chinese (Simplified)	Italian	Serbian (Latin)
Chinese (Traditional)	Japanese	Slovak
Croatian	Korean	Slovenian
Czech	Latvian	Spanish
Danish	Lithuanian	Swedish
Dutch	Malay	Thai
Estonian	Maltese	Turkish
Finnish	Norwegian	Ukrainian
French	Persian	Urdu
German	Polish	Vietnamese
Greek	Portuguese	Welsh
Haitian		Yucatec Maya

Finally, Rave holds several patents for automated update management that provides regular reminders to your communities to update contact details and alert opt-ins. When users return to the portal for updates, any new services introduced since their last login are offered as opt-ins:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Your highest priority cell phone can be listed first, and authors may then choose device targets at send time to reach the correct devices.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

System Reporting Requirements Section 4		Yes	3rd Party	Next Release	No
4.1	The EMNS must be capable of sending real time email reports to predetermined recipients. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert provides a suite of real-time reports that give the administrator visibility into the success of their notification *at the per-message and per-subscriber* level of detail, so you always know the location and success of your notifications.

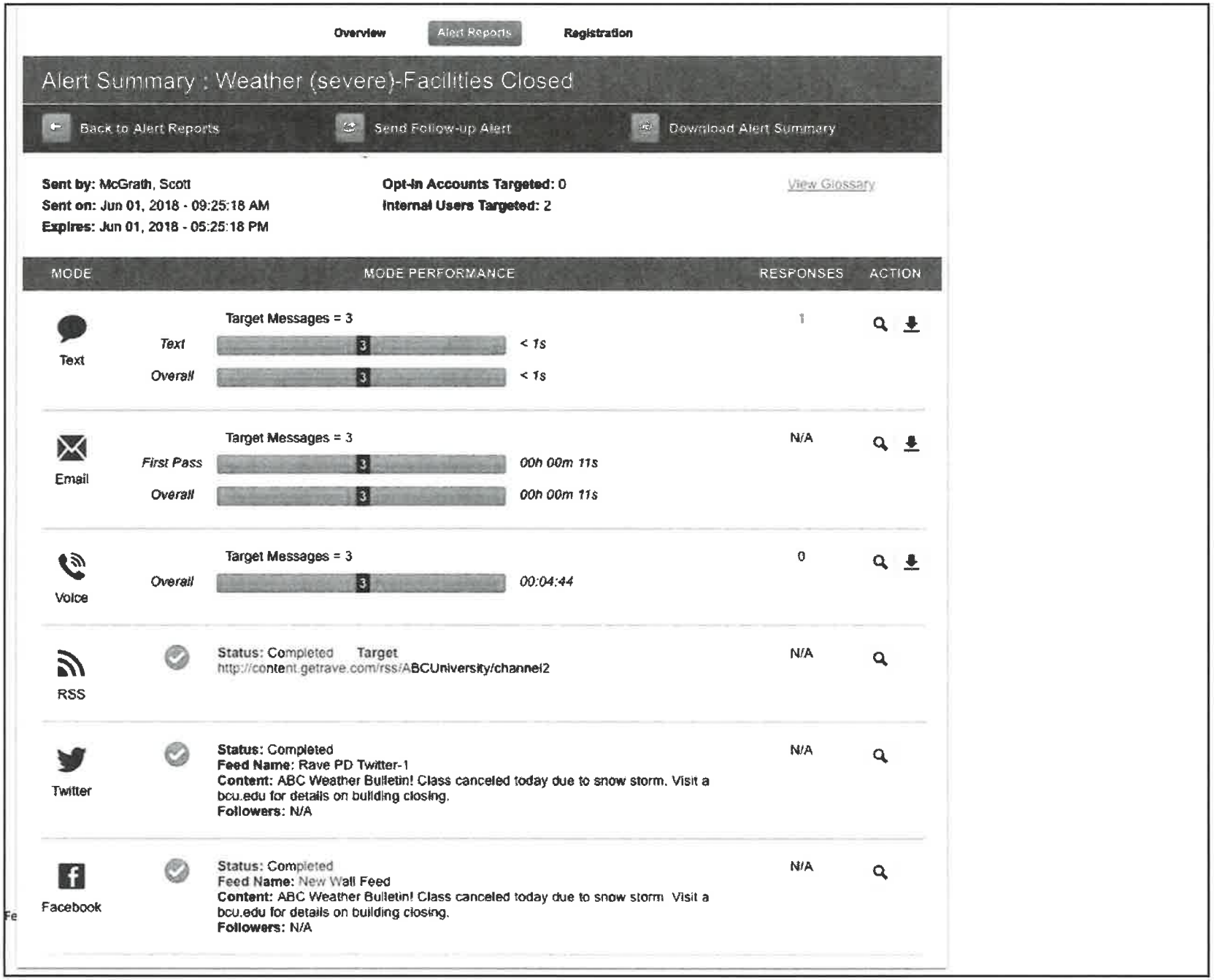
These reports include:

- **Alert Dashboard** - single console view of all Rave Alert reports
- **Alert summary reports** - provide real-time visibility into the number of messages sent by mode, messages still pending, notification successes as available, any message failures, and aggregate responses. Summary reports link to detailed reports as well as to real-time response reports; the master summary report links to a summary report targeting unique data for the delivery mode, e.g., Text/SMS, email, voice, RSS, Alertus, IPAWS, et. al.
- **Detailed alert reports** - provide user by user details on the specific notification, including number of retry attempts, timings and statistics, whether an answering machine was detected, user responses, call connects, etc.
- **Data integrity reports** - available after an alert send and provide details into delivery issues e.g. bounced email addresses, phone numbers that were undeliverable
- **Domain level reports** - provide visibility into the number of registered users, those who have validated their phone numbers, and the most popular/active groups. Domain reports also include output of Rave Alert's unique proactive contact validation processes
- **Rave mobile applications and Rave Command View analytics** - Rave's mobile applications have substantial analytics and reporting capabilities including a dashboard view, reports of Chat/Tip sessions by category, heat maps of activation points, historical reporting, case-by-case reporting, adoption statistics and similar analytics
- **Rave Prepare reports** - When selections are made via Rave Prepare queries, results may be viewed on screen, printed with rich information for field responders, and/or exported in spreadsheets that show all user contacts as well as the specific data criteria for each user's selection in the result set.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Sample Report Appearances:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Overview | Alert Reports | Registration

Alert Summary : Weather (severe)-Facilities Closed

Back to Alert Reports | Send Follow-up Alert | Download Alert Summary

Sent by: McGrath, Scott
Sent on: Jun 01, 2018 - 09:25:18 AM
Expires: Jun 01, 2018 - 05:25:18 PM

Opt-In Accounts Targeted: 0
Internal Users Targeted: 2

View Glossary

MODE	MODE PERFORMANCE	RESPONSES	ACTION
Text	Target Messages = 3 *Text* 3 *< 1s* *Overall* 3 *< 1s*	1	
Email	Target Messages = 3 *First Pass* 3 *00h 00m 11s* *Overall* 3 *00h 00m 11s*	N/A	
Voice	Target Messages = 3 *Overall* 3 *00:04:44*	0	
RSS	**Status:** Completed **Target** http://content.getrave.com/rss/ABCUniversity/channel2	N/A	
Twitter	**Status:** Completed **Feed Name:** Rave PD Twitter-1 **Content:** ABC Weather Bulletin! Class canceled today due to snow storm. Visit a bcu.edu for details on building closing. **Followers:** N/A	N/A	
Facebook	**Status:** Completed **Feed Name:** New Wall Feed **Content:** ABC Weather Bulletin! Class canceled today due to snow storm Visit a bcu.edu for details on building closing. **Followers:** N/A	N/A	

Text Details : Weather Closure

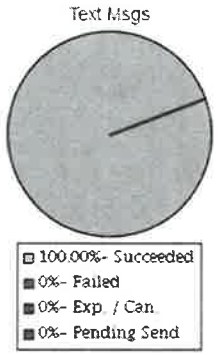
ALERT SUMMARY OVERVIEW

Respondents

Respondents	**0**	**0%**

Message Analysis

	Count	% of Total
Distinct contacts to message	**7**	**100.0000%**
Sent	0	0%
Dropped (Error)	0	0%
Dropped (Safelist)	0	0%
Dropped (Opt-Out)	0	0%
Dropped (Stop Flag)	0	0%
Dropped (Bad Phone)	0	0%
Dropped (Inactive)	0	0%
Total messages sent by method	**5**	**100.00%**
Messages sent via SMPP	4	80.00%
Messages sent via SMTP	1	20.00%



Download Text Alert Detail

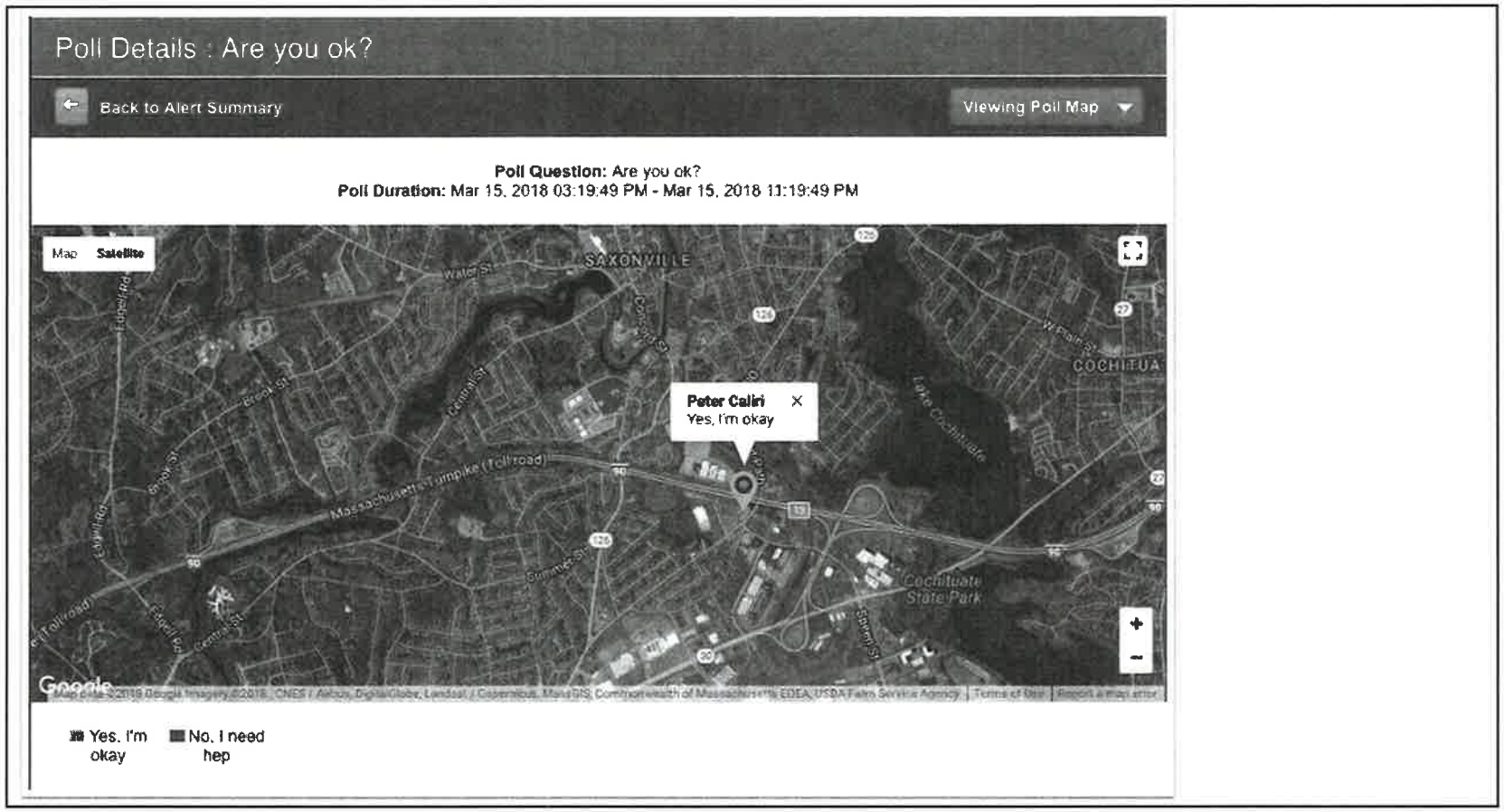
Respondents

Respondents - The number of messaged users who responded to the Text message at least once.

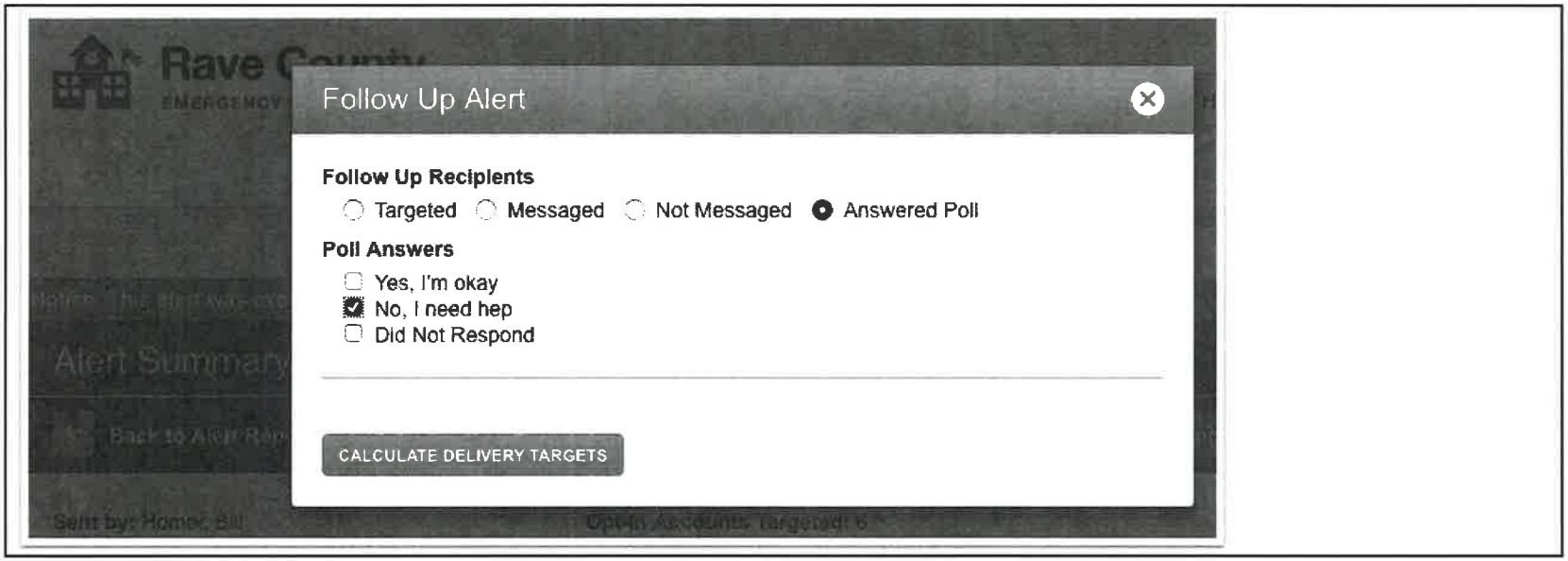
Message Terms

Distinct contacts to message - The number of Mobile contacts targeted by the Text alert, based on the selected distribution list(s) and targeted contacts.

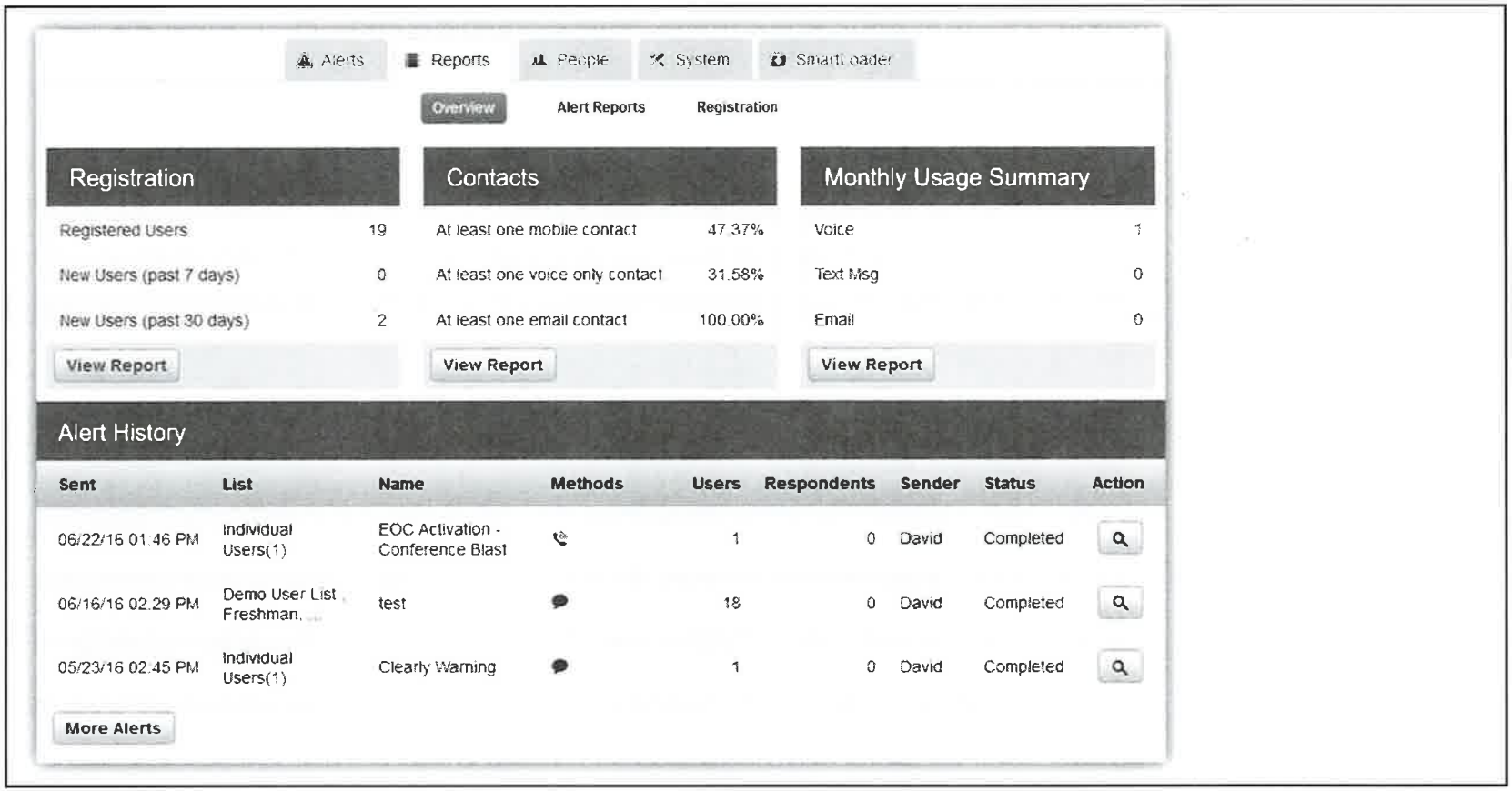
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



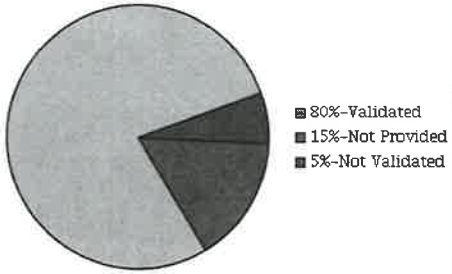
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Registration

User | Mobile | Voice | Email

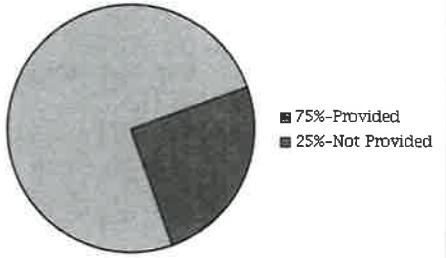
Mobile Contact (1)

Total Registered Users	**11,000**	**100%**
Provided	10,000	90%
Validated	8,000	80%
Not Validated	1,500	15%
Not Provided	500	5%
Voice Preference Enabled	**6,700**	**67%**



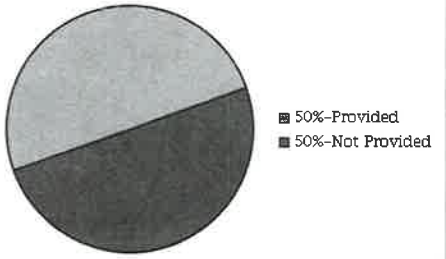
Mobile Contact (2)

Total Registered Users	**11,000**	**100%**
Provided	8,250	75%
Not Provided	2750	25%
Voice Preference Enabled	**5,500**	**50%**



Mobile Contact (3)

Total Registered Users	**11,000**	**100%**
Provided	5,500	50%
Not Provided	5,500	50%
Voice Preference Enabled	**3,630**	**33%**



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Delivery Rate Analysis	
Time to 85% delivered	00h 00m 06s
Time to 90% delivered	00h 00m 06s
Time to 95% delivered	00h 00m 10s
Time to 98% delivered	00h 00m 10s
Count of handset receipts	13

All Rave Alert reports export to CSV files, which can easily be manipulated in other software for further analysis.

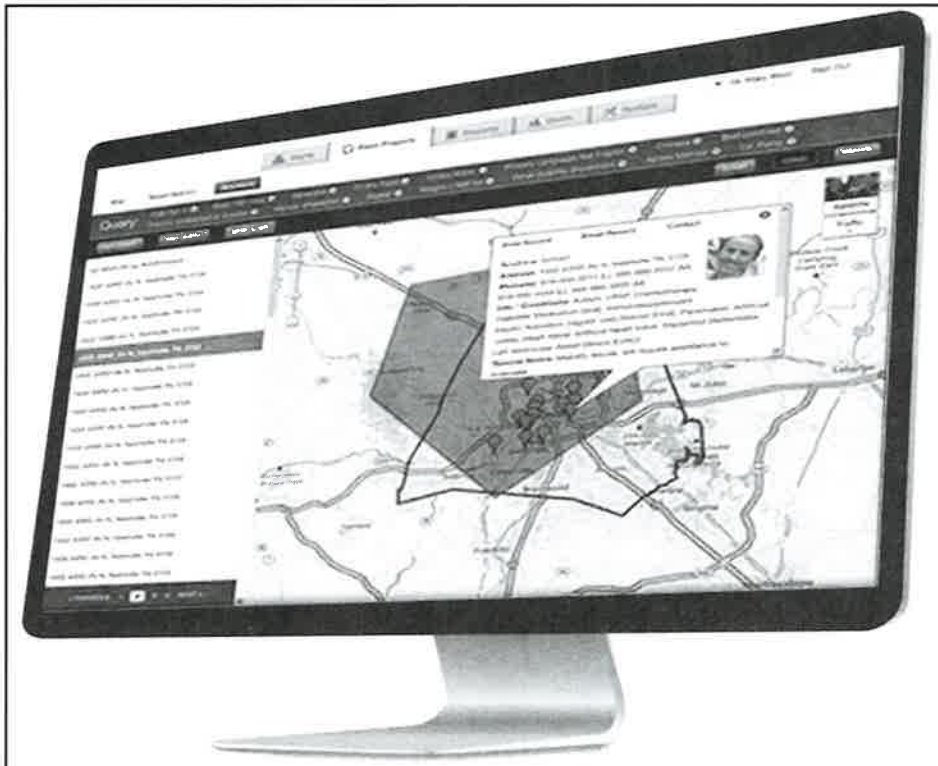
A variety of affordances facilitate custom reports, ranging from user interface controls date pickers, filters to extracted reports using customer's preferred tools Microsoft Excel, Google Spreadsheets, Apple Numbers, database and report writing tools, etc.

Additional reporting features may be available when specific Rave mobile applications are used alongside Rave Alert - for example, within WebEOC, when integrating Common Alerting Protocol with the Rave Panic Button, and others.

Rave Prepare Reporting

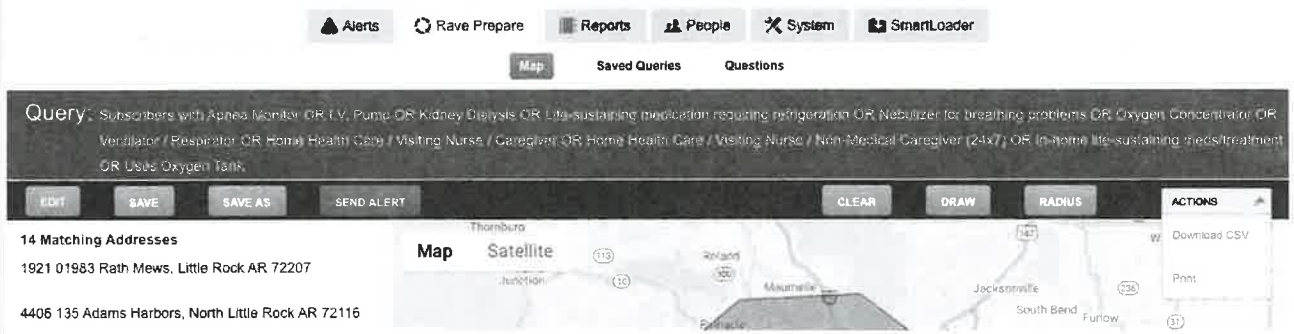
Rave Prepare is an optional specialized interface for Rave Alert that allows emergency management to run geo-spatial queries on subscriber-provided information on special access needs, functional needs, disabilities, and other specific characteristics.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Subscribers can provide this information during registration, and emergency managers use these queries to generate recipient lists for targeted notifications. Queries can be pre-saved and run against current data at any time, so your alert targeting remains accurate over time. Query results can be used instantly to initiate a message to targeted recipients in just a few keystrokes, but Rave Prepare also supports printed and exported results:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



You have the ability to save queries to run at any time against current data, or "Dynamic" queries run *ad hoc* for one-time use. When results are generated, print reports allow you to analyze and distribute this information (as well as send an alert or poll to the selected recipients):

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Smart Prepare Query Results: Jan 28, 2020 15:20 PM EST PRINT
Created By: Scott McGrath
Query: Apnea Monitor; I.V. Pump; Kidney Dialysis; Life-sustaining medication requiring refrigeration; Nebulizer for breathing problems; Oxygen Concentrator; Ventilator / Respirator; Home Health Care / Visiting Nurse / Caregiver; Home Health Care / Visiting Nurse / Non-Medical Caregiver (24x7); In-home life-sustaining meds/treatment; Uses Oxygen Tank; Within [34.775460 -92.173920, 34.858690 -92.386502, 34.652129 -92.473297, 34.766551 -92.594147, 34.572168 -92.588654, 34.597042 -92.079163, 34.775460 -92.173920, 34.775460 -92.173920,]
Matching Addresses: 14

Profile Entity	Contacts	Matching Criteria	Other
user0053 Arkansas **Address Type: Other** [redacted] **Little Rock AR 72207** Lat: 34 [redacted] Lon: -9[redacted]			
H2:hab4JB:anQ H2b0PtgY6XWTG		Apnea Monitor;I.V. Pump;Kidney Dialysis;	

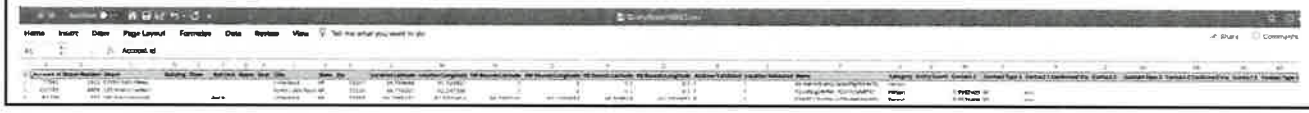
Profile Entity	Contacts	Matching Criteria	Other
user0127 Arkansas **Address Type: Other** **440[redacted]** **Nort[redacted]** Lat: [redacted] Lon: [redacted]	999-826-3986 (M)		
H2coNLgZAHMr H2iiTSTaMIP8Y		Apnea Monitor;Kidney Dialysis;	

Profile Entity	Contacts	Matching Criteria	Other
user0058 Arkansas **Address Type: Other** **215 [redacted]** **Little[redacted]** Lat: [redacted] Lon: [redacted]	999-233-2025 (M)		
H2kd0.J/6p:Hw H2Zm4e0aywhFo		Apnea Monitor;I.V. Pump;Kidney Dialysis;	

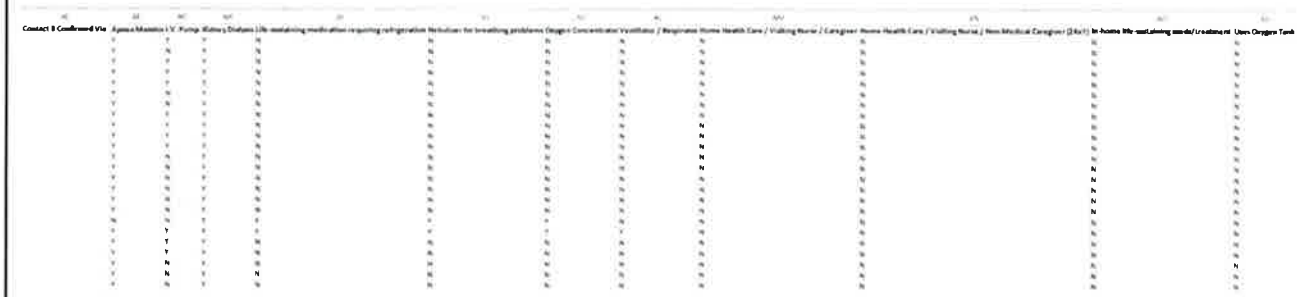
Profile Entity	Contacts	Matching Criteria	Other
user0033 Arkansas **Address Type: Other** **209 [redacted]** **Littl[redacted]** Lat: [redacted] Lon: [redacted]	999-281-3907 (M)		
H2i2NUpEcT2rk H2i5n AC8zyXw		Apnea Monitor;I.V. Pump;Kidney Dialysis;	

Profile Entity	Contacts	Matching Criteria	Other
user0040 Arkansas **Address Type: Other** [redacted]	999-537-9471 (L)		

The Export command includes user and contact information, as well as details about the specific queried attributes that selected each user in each row:



AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



		Yes	3rd Party	Next Release	No
4.2	Real-time reports of all message delivery attempts, confirmations, and polling results must be available by internet once a notification has been sent. Describe how the solution will meet this requirement.	Yes			

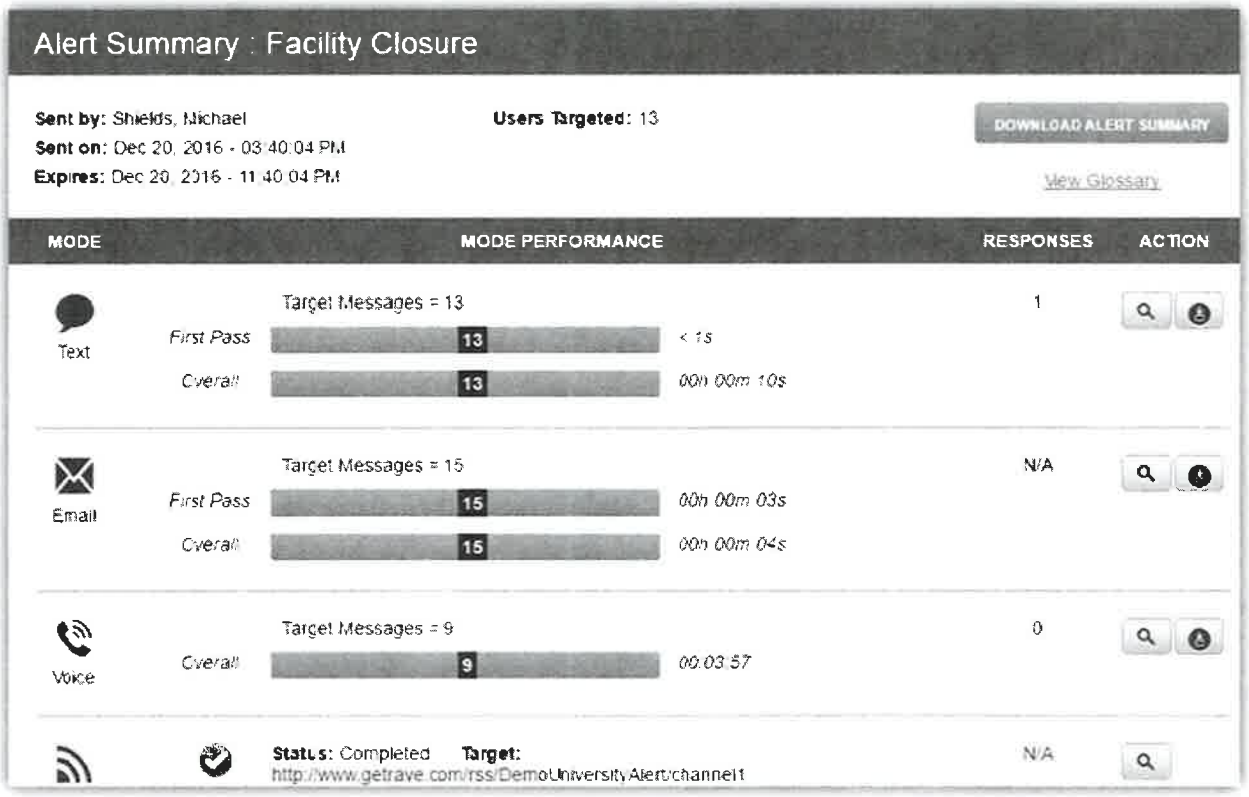
Bidder Response:

Compliant. Reports update in real-time and the report page auto-refreshes to track progress during an in-progress alert. In addition, when responses are collected - to a standard text or voice alert for example - the sender is notified of incoming responses via a push notification.

Each delivery mode displays summary data for the alert, with counters that increment during progress, and some delivery modes may use specific reporting criteria: for example, social media posts are "pass/fail" grades indicating a successful or unsuccessful

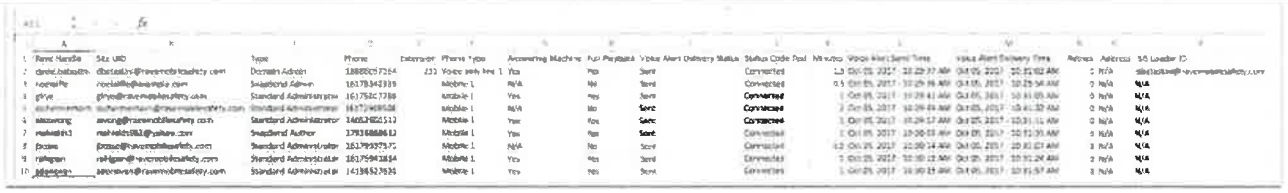
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

message post. Others, like IPAWS, show deep details about status.



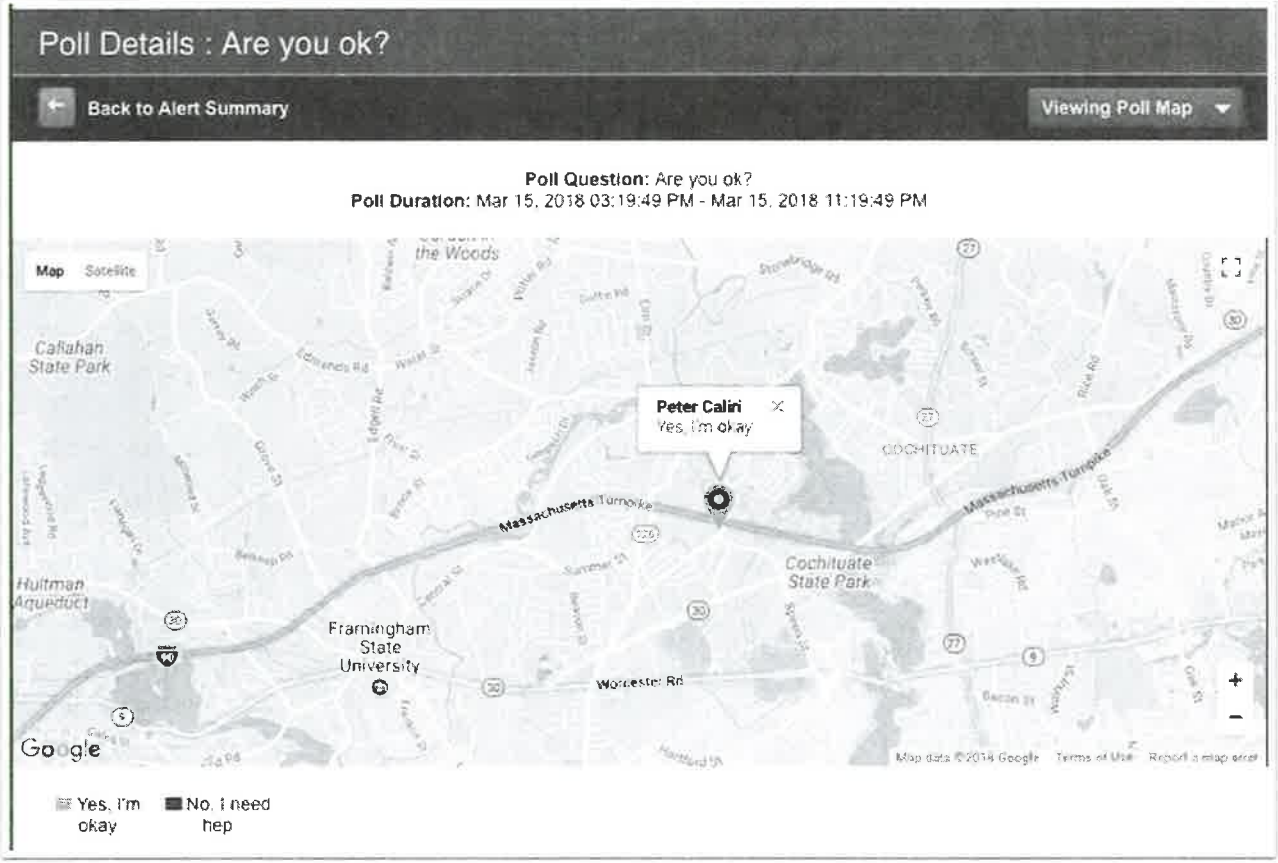
Inside each personal mode - e.g., text, email, and voice alerts - both summary and detailed information is collected. For example, email deliveries show email-specific details as well as provide user-by-user, device-by-device precise reporting for each message delivery - its contact information, send time, receive time, first pass delivery vs. deliveries requiring retries, as well as "mode-specific" details such as Full Playback status, Answering Machine vs. Live call recipient, time used on the call, the recipient's "Preferred Language" as well as the "Delivered Language" on a translated message, and more.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

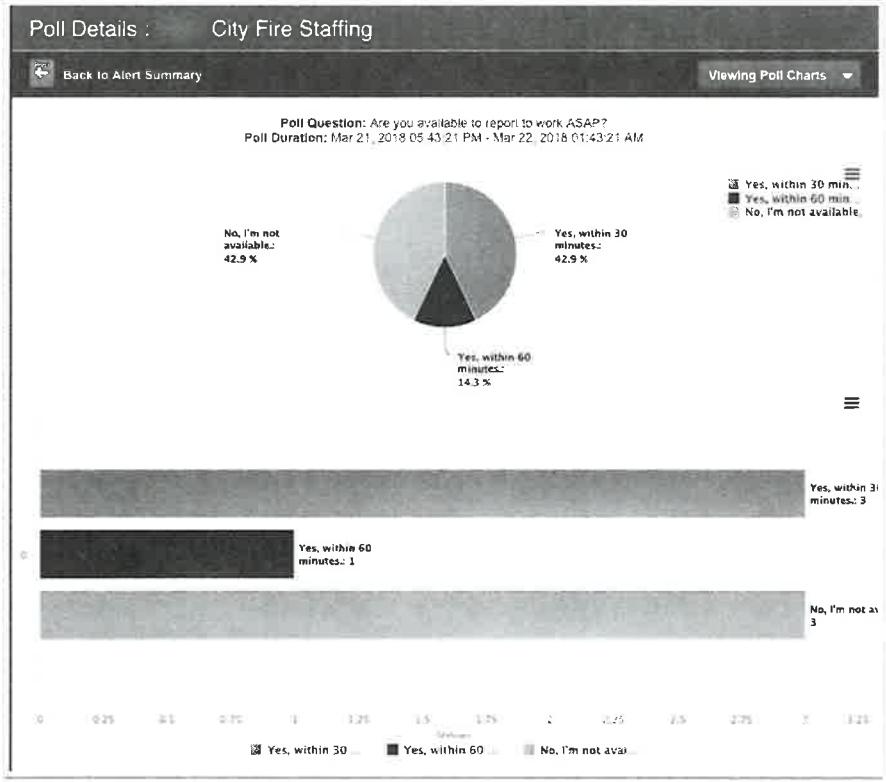


Rave's Polling Alerts have specific helpful reporting features, such as graphical and map-location views showing responses:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

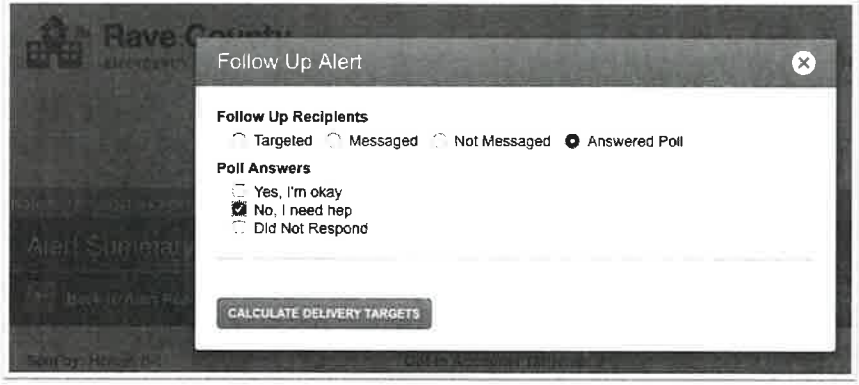


AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Once details are processed, a typical workflow is to send a Follow Up Alert, available on all notifications, to responses of a specific value:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Rave customers have often commented very positively on the attention to detail and rich transparency of Rave's reporting data in general in comparison to competitive solutions.

		Yes	3rd Party	Next Release	No
4.3	EMNS reporting must be capable of providing notification content. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. All specific content and settings are included in standard reports. For example, voice alerts include both text-to-speech used for a generated prior alert, but also support audio playback in reports that use a voice message such as IPAWS.

An additional feature extending these reports is one that allows Automatic Email Summaries to be emailed to specific admins or executive responders in order to keep critical staff, PIOs, and other key responders aware of outgoing message campaigns. These can be configured selectively. A common use case is one where a jurisdiction leader wishes to be kept aware of any public emergency communications about a specific incident.

		Yes	3rd Party	Next Release	No
4.4	EMNS reporting must be available to view or upload to other reporting databases. Describe how the solution will meet this requirement.	Yes			

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Bidder Response:
Compliant. All reports feature export capabilities; nearly all reports extract via standard .csv format spreadsheets. Several other reports and analytics include additional exporting capabilities such as image or PDF output. An optionally integrated WebEOC also aggregates incident communications within reporting capabilities tied to incident boards.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
4.5	EMNS reporting must be downloadable to a single file report delivered in a CSV format. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Standard reports provide an alert summary export via CSV; additional reports and report extracts may be available as appropriate. For example, Rave provides a daily automatically generated Enrollment Snapshot Report that extracts all critical domain user data and makes it available via SFTP on a rotational schedule. A robust description of system reporting and related functions is provided in other responses in this section.

		Yes	3rd Party	Next Release	No
4.6	EMNS reporting must be searchable by all data fields. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Many standard reports contain report type-specific filters as appropriate; for example, certain reports are appropriate for date-range searches while others may focus on heat map or other location-oriented or analytics criteria; Rave Alert's WebEOC support provisions reports that filter into incident management boards. All reports are available as spreadsheets for further manipulation and customization, importing into other systems, or other analytics.

		Yes	3rd Party	Next Release	No
4.7	EMNS reporting must be capable of providing all attempts with specific results to include: a. Recipient response action; b. Message left in voicemail; c. Disconnected; d. Busy; e. Failed notification; f. Summary of responses; g. Time notification was closed.	Yes			

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

	Describe how the solution will meet these requirements.				

Bidder Response:

Recipient response action;

Compliant.

Message left in voicemail;

Compliant.

Disconnected;

Compliant.

Busy;

Compliant. Configurable automated redials and retry wait times may be specified in voice alert profiles and/or individual alerts.

Failed notification;

Compliant.

Summary of responses;

Compliant. Shows in reports and can be extracted and used in other applications when needed, or used as the basis for a Follow Up notification based on response.

Time notification was closed.

Compliant.

Describe how the solution will meet these requirements.

As noted in other responses in this section, Rave customers often praise the extensive level of detail, precision, and overall transparency of our report details. For example, each individual delivery mode produces detailed status reporting including key

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

details for each caller, but also an overarching summary view - details for each delivery mode selected, performance, auditing and status details, and a downloadable Summary that shows all messages sent to each user.

All data elements detailed in this requirement are fully supported, as well as much more information critical to evaluation and measurement of alert details.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
4.8	EMNS reporting must be capable of providing recipient list. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

An alert summary report is the "home" view if you will of an alert campaign:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

Summary view includes targeted notification list, and the "Download Alert Summary" feature will display user-by-user detail capturing all selected delivery modes and contacts by user.

Rave Handle	Site UID	Type	Messaged	Text Targets	Text Sent	Voice Targets	Voice Sent	Email Targets	Emails Sent
mshields	mshields@ravemobilesafety.com	Domain Admin	Y	1	1	0	0	1	1
misenhart	misenhart@ravemobilesafety.com	Standard Administrator	Y	1	1	0	0	1	1
noeleiffe	noeleiffe@example.com	SnapSend Admin	Y	1	1	1	1	2	2
nwells	nwells@ravemobilesafety.com	Standard Administrator	Y	1	1	0	0	1	1
gfrye	gfrye@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
sschermerhorn	sschermerhorn@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
david.batastini	dbatastini@ravemobilesafety.com	Domain Admin	Y	1	1	1	1	1	1
alanwong	awong@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
pcaliri	pcaliri@ravemobilesafety.com	Standard Administrator	Y	1	1	0	0	1	1
mshields1	mshields962@yahoo.com	SnapSend Author	Y	1	1	1	1	1	1
jbosse	jbosse@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
rahigian	rahigian@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
adonovan	adonovan@ravemobilesafety.com	Standard Administrator	Y	1	1	1	1	1	1
mshields2	mseven86@yahoo.com	Duke Admin	Y	0	N/A	0	0	1	1

		Yes	3rd Party	Next Release	No
4.9	EMNS reporting must be capable of providing time of transmit to each device by each recipient. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Timing information is provided in summary, by delivery mode (even measuring "First Pass" delivery vs. messages delivered upon retries), for each user by each personal delivery (e.g., for email and voice), and Send Time vs. Delivered Times both in aggregate and individually.

An example: Analytics are provided in a drill-down area specific to text messages:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Text Details : Weather Closure

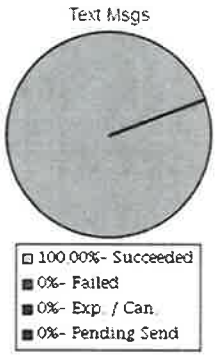
ALERT SUMMARY OVERVIEW

Respondents

Respondents	**0**	**0%**

Message Analysis

	Count	% of Total
Distinct contacts to message	7	100.0000%
Sent	0	0%
Dropped (Error)	0	0%
Dropped (Safelist)	0	0%
Dropped (Opt-Out)	0	0%
Dropped (Stop Flag)	0	0%
Dropped (Bad Phone)	0	0%
Dropped (Inactive)	0	0%
Total messages sent by method	5	100.00%
Messages sent via SMPP	4	80.00%
Messages sent via SMTP	1	20.00%



Download Text Alert Detail

Respondents

Respondents - The number of messaged users who responded to the Text message at least once.

Message Terms

Distinct contacts to message - The number of Mobile contacts targeted by the Text alert, based on the selected distribution list(s) and targeted contacts.

To make this information more actionable, this screen shows specific details for delivery:

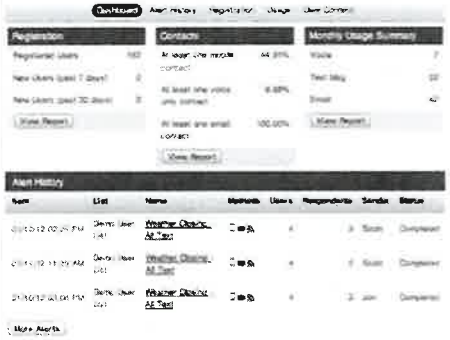
AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Delivery Rate Analysis	
Time to 85% delivered	00h 00m 10s
Time to 90% delivered	00h 00m 10s
Time to 95% delivered	00h 00m 10s
Time to 98% delivered	00h 00m 10s
Count of handset receipts	2

		Yes	3rd Party	Next Release	No
4.10	EMNS reporting must be capable of providing a detailed monthly census per division of the maximum number of enrolled contacts. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Several reports may be used for this purpose, including Registration reports that have views by data range and other parameters.



Besides specific registration reports, the product also features a daily Enrollment Snapshot report well-suited to meet this requirement.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

	Other Requirements Section 5	Yes	3rd Party	Next Release	No
5.1	EMNS must have a GIS mapping capability to enable sender to identify and outline geographic areas to receive specific notifications using at a minimum: a. Zip code; b. Radius, polygon or other pre-defined geographic shape; c. Free form, curser-drawn outline of user specific area; d. Use of pre-drawn GIS generated boundary file such as political subdivisions or other. Describe how the solution will meet these requirements	Yes			

Bidder Response:

Zip code;

Compliant.

Radius, polygon or other pre-defined geographic shape;

Compliant. Shapes may be selected during template creation or activation, may be loaded from stored shapes from our Shape Library function, or imported from standard .kml data.

Free form, curser-drawn outline of user specific area;

Compliant.

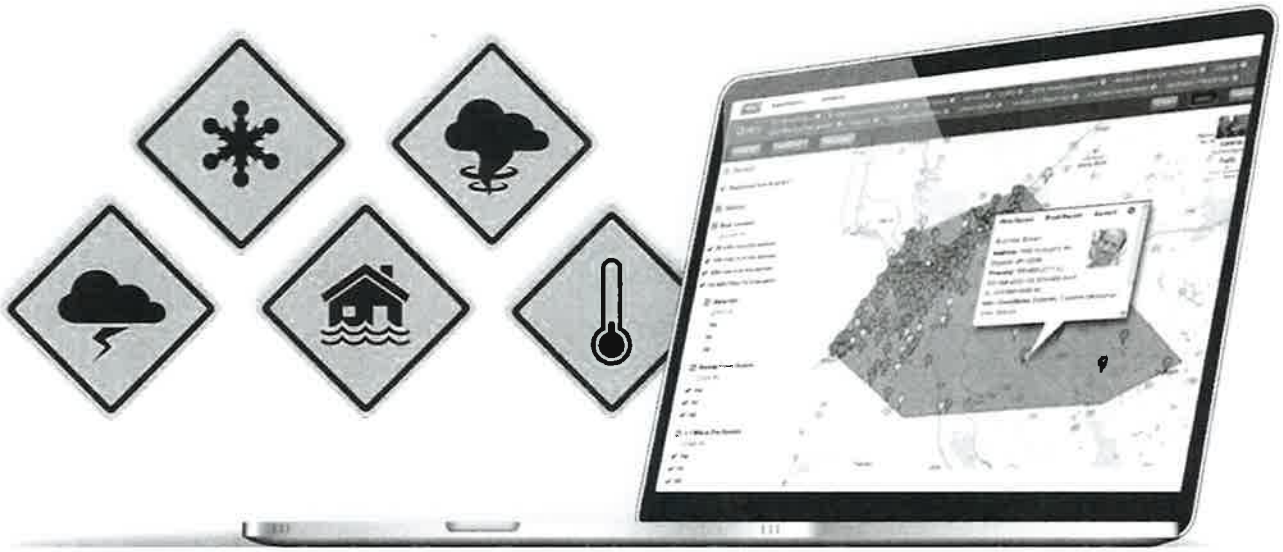
Use of pre-drawn GIS generated boundary file such as political subdivisions or other.

Compliant. Boundary data files can be imported when sending a message, creating or updating a template, added to our Shape Library for instant selection, or use when managing the geo-spatial query functions of the optional Rave Prepare functionality described in surrounding responses.

Describe how the solution will meet these requirements

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Rave Alert provides an integrated solution that enables emergency managers to systematically understand the needs of their entire community and **effectively communicate appropriate messages** to defined segments within their communities via multi-modal notifications using geographic selections. We provide a mapping interface with polygon, radius, and similar drawing tools to facilitate geographic selection. In addition, the product contains a powerful, access-controlled, re-usable Shape Library function.



Geo-targeting Via Standard Data Sources

One way to get geographic targeting data is by loading known databases, like landlines and other premise-based communications. Rave Alert supports provisioning landline and premise-based communications for geo-targeted selection from a variety of potential sources - client-provided data (e.g., from GIS systems); MSAG, ALI or similar white / yellow page sources.

Rave Alert supports an optional feature for loading geo-tagged address-based contacts that can be geo-targeted within the user interface. The process involves an extract of contacts from your GIS systems or provisioning from other data sources. Each update is a complete refresh of the data, but a persistent exclusion feature supports number blocking when needed, and persists over multiple data refreshes.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

Geo-targeting Via IPAWS Notifications

Rave Alert provides full support for IPAWS notifications. The customer must be authorized by FEMA, with an executed Memorandum of Agreement (MoA) from FEMA, as a Collaborative Operating Group (COG) in order to use IPAWS technology features in the product. When approved, Rave installs the certificates provided by FEMA to the customer's alert configuration.

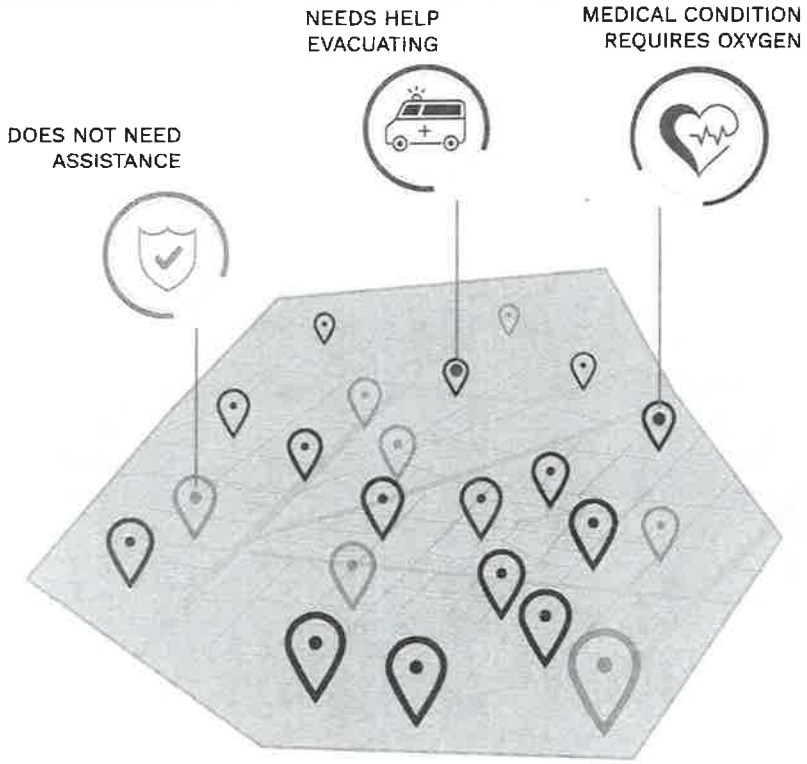
IPAWS messages can, when necessary, be fully configured at runtime in a user-friendly, guided user experience. The administrator creating an IPAWS message will see only validated values within the user interface. In typical usage, however, messages are pre-configured in alert templates to support specific emergency plans, and then the administrator can update the message content to be customized before sending when necessary. Map data provided to target your jurisdiction will be validated to ensure it meets FEMA's standards.

Rave Alert fully supports a test configuration against FEMA's IPAWS Labs Cloud test environment within standard configurations.

Geo-targeting Via Subscriber Provided Information

On our secure online registration portal, subscribers can enter addresses that are important to them, like home and work locations. Each subscriber can add unlimited addresses, and set preferences about how and for what situations they'd like to receive alerts related to these addresses. They can also self-identify vulnerabilities and special needs for them and their families, associate this information with particular addresses, and choose to share it with emergency management. The system automatically prompts them to update this information quarterly, providing you with an up-to-date, geographically targetable database of specific need groups that you can use to send alerts:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Rave Alert validates address data in multiple dimensions. A "clean address" is offered to the subscriber as an alternative (accepted by more than 95% of users in real world statistics), and a view of the address pin is provided on the map along with instructions to relocate the pin if the standard map source is slightly inaccurate.

Since this data is intelligently integrated to a GIS mapping system and an emergency notification system, emergency managers can quickly identify, locate, and communicate with individuals or groups as needed using our map interface. They can also view this subscriber-inputted data during emergency planning to better gauge the needs of their community. This gives you unparalleled

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

insight into the special needs and geography of your diverse community. Armed with this insight through Rave Alert, you can allocate the right resources during planning, and get the right message to the right person through their preferred communication method during an emergency.

Public Registration for Residents Without Email

A common issue encountered in public notification subscriptions is supporting community members who do not have email accounts or rely on assistance from others to register for notifications. Rave's public portal platform provides specialized support for your communities facing these issues.

The portal enables email-less registration that allows citizens to register using alternative contacts, like phone numbers. This feature set improves program inclusiveness by removing a substantial barrier to entry for public notifications. It supports three critical capabilities:

- Allows citizens to create an account using a phone number, where they can sign up for notifications, provide vulnerability data, and manage preferences
- Allows citizens to provide contact information of an "Assistant" who can help them sign up for alert services, keep account information up to date, and receive account maintenance communications
- Allows citizens to recover forgotten account credentials without requiring an email address

Geotargeting Mobile Applications

Rave's mobile applications for alert recipients allow "geo-targeting" of notification recipients. App users who permit location features on our mobile applications can be reached via a geo-graphic selection, alerting only those application users who are currently within a geographic boundary managed by the alert sender using our standard mapping interfaces and reusable Shape Library. During the (configurable) duration of the notification, application users entering the boundary of an active notification will be notified upon arrival within the perimeter.

Targeting Flexibility Rave Alert's targeting options can be combined, allowing your administrators to add geographic selections to traditional lists or other grouping mechanisms like queries to ensure the proper recipients for a particular alert. We also support polygonal weather alerting, which automatically targets recipients with GIS-data within the affected area of a weather event.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
5.2	EMNS must have automated National Weather Service (NWS) alert capabilities available. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert can apply a number of filters against National Weather Service weather notifications; the recipients for a given alert weather alert notification can be selected based on the values enclosed within a wide variety of customer-defined rules, including severity, urgency, category, event code, location, etc. Notification selections can be determined by weather type and severity, and/or by weather events that fall within a specific geographic area.

A variety of options allow you to configure weather messaging to all users, a small group of responders who may evaluate the need to rebroadcast conditions, or an opt-in group specifically requesting weather notifications, individually by type of weather event if required. Weather notification rules can also declare quiet hours for specific weather types if desired.

Rave's citizen mobile app also supports configurable location-aware weather messaging options, as part of its standard features:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Figure: Sample Community Marketing brochure, part of Rave's Community Marketing toolkit.

		Yes	3rd Party	Next Release	No
5.3	The EMNS must have a minimum of at least two language translation capabilities to include English and Spanish. Describe how the solution will meet this requirement. If more are available, list in the space provided below.	Yes			

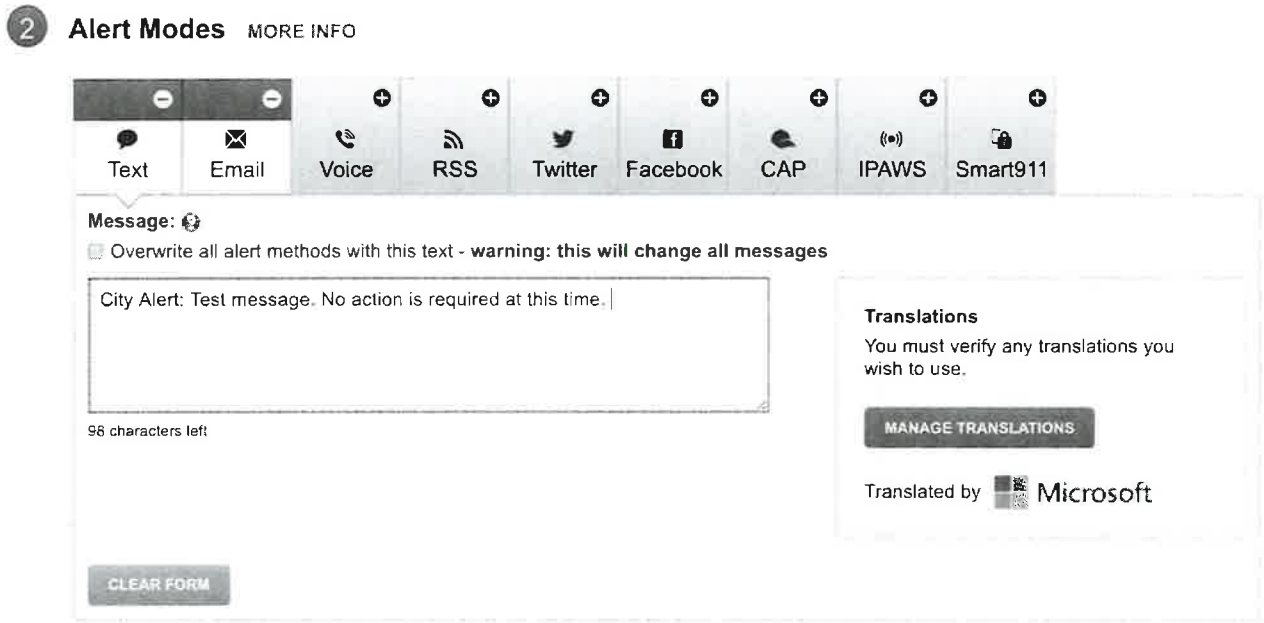
Bidder Response:

Compliant. Rave Alert supports multiple languages for outbound text-based alerts with automated translation into up to 62 languages.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.
AT&T Business

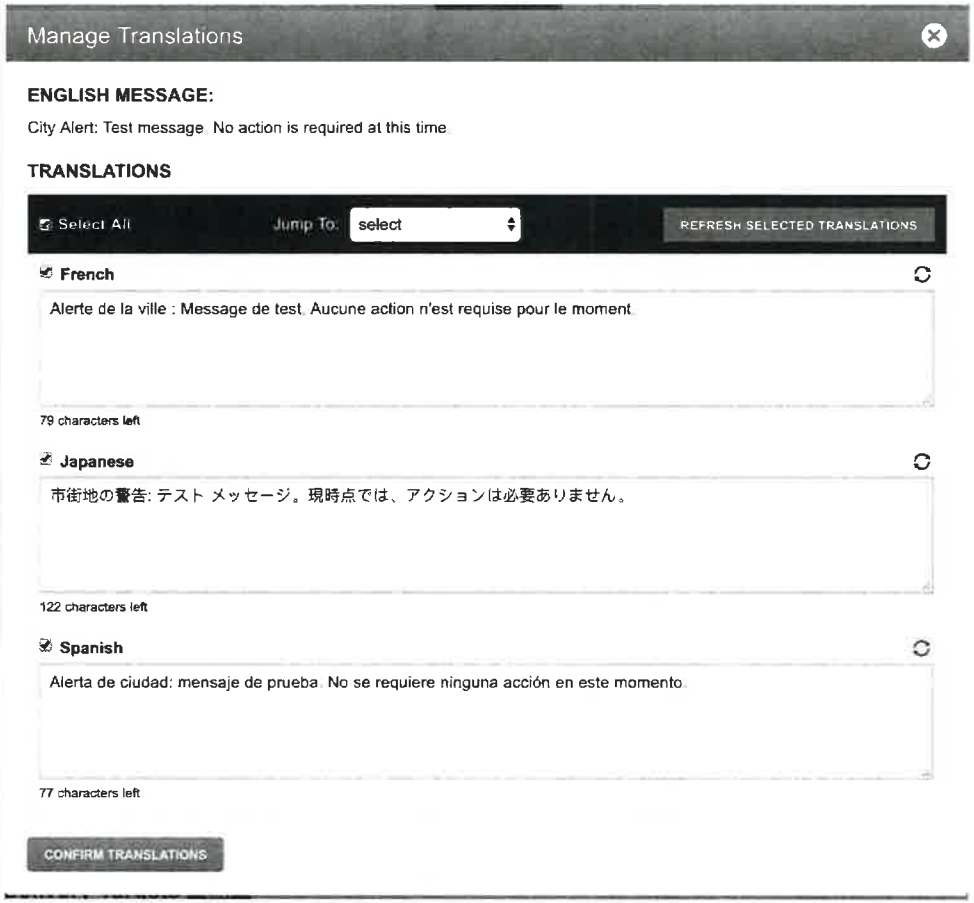
Within our organization-branded self-service portals as well as our recipient mobile apps, subscribers can specify a preferred language. You can also programmatically upload preferred languages stores in staff or other databases through our bulk loading tools and/or our User Management API. For each alert where the preferred language translation is provided, the user will automatically receive messages in that language. If a translation is not provided the user receives the English message.

When configuring an alert, alert authors can auto-translate alert text into any of our supported languages. These translations also support editing and saving to permanently correct auto-translation errors.



Inside an alert template, a Manage Translations button appears on Text and Email messages. This button opens the "auto-translate" interface; customers may also override manual translations if desired.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.



Once translated messages will present translated content based on the user's preference.

Automated translation of outgoing alerts are configurable for the following languages:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Arabic	Hebrew	Queretaro
Bosnian	Hindi	Otomi
Latin	Hmong Daw	Romanian
Bulgarian	Hungarian	Russian
Catalan	Indonesian	Serbian Cyrillic
Chinese Simplified	Italian	Serbian Latin
Chinese Traditional	Japanese	Slovak
Croatian	Korean	Slovenian
Czech	Latvian	Spanish
Danish	Lithuanian	Swedish
Dutch	Malay	Thai
Estonian	Maltese	Turkish
Finnish	Norwegian	Ukrainian
French	Persian	Urdu
German	Polish	Vietnamese
Greek	Portuguese	Welsh
Haitian		Yucatec Maya

Character compatibility depends on encoding features enabled on a user's mobile device, email client or web browser. Typically, subscribers configure devices to support their preferred languages.

Also, Spanish language is supports for both 90- and 360-character fields in WEA 2.0 messages sent via IPAWS.

In addition to email and text translations, text-to-speech *voice* translation is being enhanced to support 8 languages in Rave's 2020 product roadmap.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
5.4	The EMNS provider must have provided similar services for similar sized customers for a minimum of six (6) years. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

****AT&T has worked in the public sector of the State of Nebraska ...

Rave Mobile Safety's platform has a track record of real-world tests from our 15 years providing ENS systems to 6,000 public city, state, county, local government, and agencies, as well and many higher education clients (including the University of Nebraska) and healthcare and hospitals and business customers serving millions of subscribers.

Rave began building our mass notification platform to support the unique demands of high volume higher education emergency notification. We work with nearly 2,000 higher education institutions, including a large majority of large public and private universities such as the University of Nebraska, University of Wisconsin, The Ohio State University, and Indiana University, where these institutions have a large population living in a densely populated campus environment. Our first lessons as a service provider were focused from the start on building a robust, redundant, high availability and high-performance environment built to notify tens and hundreds of thousands of subscribers with critical safety communications in just minutes.

Our government practice initially rolled out in 2011, and over time, our features have come to expand to include many feature areas that are critical to public notifications, including:

1. A robust, user-friendly **public subscription portal** to support accessible, inclusive citizen and resident participation.
2. Location features specific to **geographic targeting** for public subscribers, public data sources like ANI/ALI and GIS data, and mobile app push notifications based on real-time location and using Wi-Fi to reach users who may be unable to connect to cell towers.
3. Strong support for **IPAWS activation** and updates to WEA messaging, with careful attention to user interface features that support activators often managing very complex incidents.
4. **FedRAMP certification**, due in early Q2'2020.
5. **Rave Prepare™** - an optional product feature area to support optional provisioning of information significant to responders and emergency managers concerned with inclusive incident management that supports residents with access and functional needs, people with disabilities, and other specific information of obvious benefit during preparation and response phases of your OEMs. Rave Prepare can run geographic queries combining jurisdictional locations and specific information

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

needs - e.g., residents in a flood area who depend on electricity to support medical equipment or who may need assistance during an evacuation - and then message those residents directly based on those needs.

6. **Mobile applications for recipients** - Our portfolio of mobile applications grows. Our public recipient app provides a complete user-friendly alternative to our web portal for managing subscriptions and specific alert category opt-ins, and to provide a scope that allows even visitors from outside the area to see your public alerts or even receive push notifications when in an area selected for geographic notifications targeting app users.
7. **Automated** geography-based **weather notifications** - Configurable in many ways to manage weather communications to Emergency Managers for watches and opt-in subscribers for serious warnings and evacuation notices.
8. **Optional SMS Opt-in keyword** subscriptions can be used to provide very low friction opt-in, either for the long term or during a specific event for a certain number of days or up to a given date.
9. Rave has a strong technology partnership with Juvare in support of the ubiquitous **WebEOC™ incident management platform**. Juvare supports a Rave Alert Extension for WebEOC that can fully integrate Rave Alert notifications with your incident boards.
10. Effectively partitioned use models for **internal notification scenarios, operational notifications, callouts and dispatch communications**.
11. Innovative integrations with other public safety functions. These include the **Rave 911 Suite**, known in communities as the Smart911™ brand, tools that turbocharge 9-1-1 call response with extensive functionality ranging from caller profiles, automated outbound text chat for disconnected or interrupted calls, and access to facility information provided via Rave's free RaveFacility.com service. The **Rave Panic Button™ mobile application** is used in several statewide implementations and many very large school systems, courthouses, public offices, and other institutional properties to reduce response time to emergencies by notifying local responders and impacted staff near an incident while a caller requests public safety responses from 911 services. For example, during a medical emergency, your CPR-trained staff can be notified of a nearby person in need of an AED while 911 dispatches EMS to the site.
12. **Access control** features to manage *complex organizations and jurisdictions* effectively and in a safely delegated fashion.

Proven Reliability

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Rave Emergency Notification is designed for stress. During the Boston Marathon bombing and Super Storm Sandy Rave Emergency Notification delivered millions of messages to a wide range of recipients.

- Availability -- Backed by geo-redundant data centers our infrastructure ensures high performance and 99.999 availability
- Redundancy/Failover - Live connections to multiple wireless carriers and Tier1 SMPP aggregators keeps messages moving in every stress environment.
- Security - Our data centers are SOC2 compliant and complete regular 3rd party security audits.
- Access Control - System access controlled by role-based permissions. This allows you to empower your team with appropriate levels access and execution.
- Easy set up and maintenance -- Software-as-a-Service SaaS - Hosted, branded, web-based solution requires no on-site installation or maintenance is rapidly deployed and configured to your specifications

Rave Mobile Safety's platform has a track record of real-world tests from our 15 years providing ENS systems to 6,000 public city, state county, local government, and higher education clients.

		Yes	3rd Party	Next Release	No
5.5	A monthly test of each message delivery mode to at least twelve (12) or more recipients by each political subdivision must be included at no additional cost including any new political subdivision subscribers added after the start of the contract. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave's licensing is for unlimited testing with the system without restrictions on message volume or content.

		Yes	3rd Party	Next Release	No
5.6	The proposed EMNS software must be quoted and be supported as a standard existing and working product from the contractor, not as custom programming. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Rave Mobile Safety provides our hardened and proven platform hosted, cloud-based product set with a large list of standard features that are available standard; integrations are performed using standard methods such as RSS, CAP, data management ETL, and authentication integration - but by configuration, not by custom programming.

Supporting over 6,000 customers, Rave has built a sustainable product set by listening to customers and prioritizing our product development based on the many workflows, requirements, and features that serve the needs our customers share as common priorities.

		Yes	3rd Party	Next Release	No
5.7	The system should be simple to use and should not require extensive training. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. One common theme we experience when migrating customers to our platform is our ease of use. With ease of use comes a low cost and effort to train.

Comprehensive Training for Unlimited Administrators and Alert Authors
Your Rave Alert implementation comes with comprehensive initial and ongoing training for your system users. We will deliver initial training sessions to your domain administrators, and we hold regular scheduled training, live or pre-recorded, that is open to all customers. Training is available to your administrators via live sessions, an in-product training mode, and on-demand online materials. These training offerings are included in our standard services commitment, and have no additional cost.

If requested, we can also provide on-site training during implementation, which does have an additional cost. Generally the system's ease of use makes off-site and on-site training equally effective.

For typical alert activation, most administrators use 1-2 hours of online courseware and live training to be ready to leverage the full power of Rave Alert's system. Alert Authors with less administrative control can usually be trained in a matter of minutes, due to the intuitive user-experience of the product.

Provided training materials include:

- Rave Alert FAQs: User Console - commonly encountered questions on creating and sending alerts
- Rave Alert Management Console Guide - support geared specifically towards managing

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

- Rave Alert User Guide
- Rave Alert Group Administrator Guide
- Specific feature "Viewlets" - quick, targeted support for specific features, for example "Using Geo-Targeting Alerts"
- Customer webinars - highlight areas of the platform and new features, timed with releases
- Unlimited access to the Rave Academy - online learning management system with self-study courseware
- Unlimited access to Rave's Customer Support portal

For external integrations, for example IPAWS, a training process outside of Rave's products may be required. Rave recommends complementing our IPAWs related support with online IPAWS training provided by FEMA.

Training Mode

Alert Authors can enter Training Mode at any time through our web-based administrative interface. Training Mode enables all Rave Alert tools except alert broadcasting abilities, so users can practice directly on the interfaces they will use to send alerts.

The Rave Academy

The Rave Academy offers general overview videos and short tutorials targeted to specific features and a certification program. Customers and their administrators have unlimited online access to the Rave Academy at no extra cost. In addition to these resources, Rave's Customer Support Portal offers a variety of self-help training materials, recorded versions of live training sessions, helpful documentation, and other information. Onsite training options are available at an extra cost; please see pricing for details.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Customers typically self-manage oversight of training utilizing online resources. The Rave Academy learning management system supports a variety of topics for self-paced study. Administration of the system is covered within short video tutorials on our hosted learning management platform, available 24x7.

Training ranges from 30-minute to 90-minute self-study courseware options, depending on features utilized. A certification process can be used if the customer wishes to require it of alert authors and administrators.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

This is to certify completion of the training courseware for

Alert Administrator Course

Training Course for Rave Alert and Rave Messenger

This Certificate is Awarded to

Alicia Admin

Completed On

January 7, 2015

RAVE

The Rave Support Center

The product is also well supported by extensive documentation. Rave Alert links to the Rave Support Center on every page of the administrative interface. Features of the Support Center include:

- Complete online help system for the administrative user interface
- A searchable knowledge base of helpful information and product FAQ
- Links to the Rave Academy and all other instructional tools available to administrators
- Materials for customers who require "train-the-trainer" style content for local instruction
- Best Practices documentation
- The Rave Alert Subscriber Marketing Toolkit
- Best Practice Guide for Configuring Role-Based Access Controls (RBAC)
- Detailed technical documentation covering all integration points
- "What You Need To Know" section
- Product Update information and Release Notes for past and upcoming releases

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Premium Support and Training Options

We also offer cost-optional services where we can send a Rave expert to your campus at points after implementation, so they can teach you about new features since your purchase and improve system optimization.

This optional offering brings a Rave product expert on-site to work with your team, match your needs to new features, help configure access controls that match your departments, and more. Then, our expert runs training sessions for any number of alert authors and domain administrators, covering both basic and advanced configuration topics.

Prior to each Premium Support visit, your instructor consults with you to prepare and customize the curriculum to match you customer's specific requirements. The agenda will typically include a selection from the following:

- Review overall project implementation and notification policies and procedures
- Workshop to configure optimal role-based permissions and other product configuration defaults and options, workflow
- Group management
- Optional IT discussions if needed to discuss integrations
- Tiered on-site training sessions:
    - Alert Author training - basic usage of core product features for activating notifications with the product, using the product on mobile devices, and using the 24-hour emergency hotline when needed
    - Advanced Administration topics - Hands-on training for Domain Administrators covering a wide range of configuration and tools.

Once agreed upon, a Statement of Work (SoW) is executed to initiate the project and schedule site visits

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

		Yes	3rd Party	Next Release	No
5.8	The bidder must identify who controls or owns the product. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Rave Mobile Safety owns and operates all components of the safety platform. The MLSA attachment provides a full detailing of service level commitments, but fundamentally, service obligations impacting product availability, performance, and maintenance are included as part of the Rave platform infrastructure, including hosted services, operational support, and software upgrades, patches and updates that impact platform functionality. Rave Mobile Safety also provides technical support for all administrative/activator users of the system, as well as providing end-user support for public self-service portals. The customer is responsible for overall policy governance of the solution, such as usage guidelines, training compliance with product and related disciplines (such as mandatory training requirements for access to IPAWS), message activation, subscriber account support, and other communications uses to which Rave Alert will be put. Account support will be managed by AT&T and Rave Mobile Safety in partnership.

		Yes	3rd Party	Next Release	No
5.9	The bidder must identify what components or elements are leased or partnered. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. AT&T provides account management and contracting options for this bid. Rave Mobile Safety maintains platform-level relationships with a variety of network providers - wireless and wireline carriers, public email providers such as Comcast, Google and Microsoft, and with a small number of technology partners often integrated with our notification tools. Two primary examples are Juvare WebEOC and Alertus, Inc. Both vendors provide their own tools that are common integrations with Rave Alert.

All components presented by Rave are featured on the Rave platform, and all network provider relationships are part of our platform support, fully hosted managed services.

	Yes	3rd Party	Next Release	No

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

5.10	The bidder must identify who owns the elements that are leased or partnered with. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Leased or partnered technologies are not required outside of integration to on-premise systems. The Rave Alert Extension for WebEOC is a separate product licensed directly from Juvare, Inc.

		Yes	3rd Party	Next Release	No
5.11	The contractor must not require the State or any agency subscribing to the Service to purchase any new additional hardware, software or maintenance to sustain functionality. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Rave Alert is a fully cloud-hosted software-as-a-service product and does not require any onsite hardware or software installation. All functionality scoped within this bid is included unless otherwise noted.

		Yes	3rd Party	Next Release	No
5.12	All bidders must include in their proposal response a description of the proposed method of importing the current user data from the current EMNS. Describe how the solution will meet this requirement.	Yes			

Bidder Response:

Compliant. Your Rave Client Manager will work with you to perform any needed migration support from other notification tools as part of a clean and straightforward onboarding process.

A variety of migration strategies may be applied based on specific use models of data from your outgoing system. First and foremost is to preserve and manage "opt-ins" where users have granted permission to receive alert notifications. In some cases, a strategy of re-confirming participation based on migrated user data can be an effective way to manage ambiguous or imprecise consent or opt-in behaviors from past activities and systems.

In all migration discussions, a key condition for the customer is that all migrated data is "owned" or fully licensed by the jurisdiction. Rave recommends examining the data ownership and portability supported by current systems.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Sourcing of ANI/ALI data from 9-1-1 public sources can be managed in several ways, again based on customer preference and data availability. Some jurisdictions prefer such data extracted from customer GIS data sources; many others will utilize data provided by wireless carriers or CAD system vendors; Rave can also license such data on behalf of the customer as a purchasing option.

Rave Alert offers multiple tools to accept data from different database used for employees, staff and other key persons protected by our systems:

SmartLoader
Rave Alert offers a suite of batch-oriented data automation and ETL capabilities called SmartLoader. In Rave Alert's batch interface formats, a CSV file-based upload process supports a full contact upload as well as segmentation of users into messaging groups.

You can use SmartLoader to automatically:

- Add new users to Rave
- Opt users in to Broadcast Alerts via e-mail, text, and voice message depending on provided device contact information
- Remove members from Rave who do not appear within the batch file
- Update attributes such as phone and email contact information associated with existing users when re-running an updated batch file
- Create and manage groups and group properties
- Manage group subscriptions

SmartLoader can be configured to automatically update and sync data with other databases as personnel information changes.

Over 35 points of validation are supported by the SmartLoader utilities, including scanning for duplicate records. For example, Rave Alert validates both mobile carrier and whether a specific mobile number is in service. This implementation provides a "set it and forget it" style of ongoing management of subscriber data in and out of the ENS.

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Managed Contacts

Rave Alert also supports broad functionality for manually loading contact information for guest or temporary users using our Managed Contacts feature.

Managed Contacts lets you create, edit, and delete user records by loading a CSV file, with the ability to specify start and expiration dates, multiple contact points per user, group affiliations, and geo-tagging and address data for contacts for use with geographically targeted notifications.

User Management API

The Rave User Management API allows for management of subscriber data, group properties, and much more, directly from within bespoke applications such as portals and personnel systems. It is a robust user management API that can support real-time user management via our REST API. The API also supports all list and group functionality in the product, as well as optional interactive services supporting two-step mobile phone confirmation flow. Manual management tools for help desk or other administrative users with assigned permission levels, are also available.

These APIs also support messaging to individual recipients by SMS and voice, allowing you to embed notification functions in response to application events. This feature is not designed for mass notification.

HR Systems and Other Databases

Rave Mobile Safety has experience integrating with a wide variety of HR systems and other databases using the tools described above. Update schedules are configured based on customer needs, with data refreshes performed anywhere from daily to yearly.

		Yes	3rd Party	Next Release	No
5.13	Bidder must make initial training available for administrators and message initiators available for each division of the EMNS. Additionally the bidder must provide additional online administrator training to account for turnover and growth to each division at least twelve (12) times per year as needed. Describe how the solution will meet this requirement.	Yes			
Bidder Response:					

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Compliant. Response 5.7 above details the many training and support tools that Rave provides as part of our product set. The majority of our customers find that the default Rave Academy and related training content are more than sufficient. However, premium on-site training offerings are available, providing proficient Rave trainers working on site with staff. We also offer options to develop a custom curriculum on the Rave Academy or "train-the-trainer" materials that can be adapted and adopted across your organizations. These options would be determined via a lightweight Statement of Work (SoW) that capture required training needs, length and quantity of engagements and more.

AT&T provides the world-class support trusted by thousands of public agencies across the US, as it brings together many emergency management and emergency response technology in 9-1-1 centers. AT&T also services the national contract for the FirstNet network supporting priority communications for first responder agencies.

Rave's Customer Success Team and the annual Rave Summit User Conference

Rave's commitment to our customers reaches far beyond the onboarding process. Rave's dedicated **Customer Success** team that is responsible for periodic check-in reviews, supportive discussions of features and best practices, and problem-solving and customer advocacy when needed. They represent the voice of the customer across the entire Rave Mobile Safety organization.

The highest compliments we receive from our customers, the ones that make us most proud, are about our relationship with our customers, how well we listen, how collaborative we are, how hard we work to understand the everyday work done in all jurisdictions, and how innovative we can be with solutions.

Rave's Customer Success team is charged with periodic Executive Business Reviews (EBRs), as well as to check in with customers to gather feedback, review or troubleshoot issues, suggest new features and best practices, and to act as a conduit to all interaction with Rave Mobile Safety.

The Customer Success team also supports our annual user conference, the **Rave Summit**. In 2020, for the first time, Rave will support two Rave Summit events - in March in New Orleans, and in Boston in November. The 2018 Rave Summit was held in Denver in April 2018, and in Orlando, Florida in April 2019. More information about the Rave Summit can be found at

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

www.ravesummit.com.

In addition to our annual conference, Rave Mobile Safety also supports regional user group meetings around the US, where customers can network, share ideas and best practices with peers and peer organizations, attend training sessions, interact with key Rave staff, provide direct product feedback, hear keynote addresses, participate in panel discussions and more. In 2019, User Groups were held in two locations in Massachusetts, at the Emergency Operations Center in the City of Chicago, and in locations around the country such as Houston, Seattle, Virginia Beach, Oakland MI, and in other locations. Rave Customer Success is planning 10 regional user group events in 2020, in addition to our Summit conferences.

Appendix

AT&T Proprietary: The information contained herein is for use by authorized persons only and is not for general distribution.

Cost Proposal
Request for Proposal Number 6214 Z1

Bidder Name: AT&T

Cost submitted for Year One, Year Two and Year Three of the initial period are firm for the entire contract period each year and cannot increase. Price escalation of no more than 3% may be allowed for each renewal period.

Any request for an increase must be submitted in writing to the State Purchasing Bureau a minimum of 30 days prior to contract renewal date, and must show cause and be accompanied by supporting documentation. Failure to supply any requested supporting documentation may be ground to reject the requested increase and cancel the contract. The State further reserves the right to reject any proposed price increase(s), cancel the contract and re-bid if determined to be in the best interest of the State. The State will be given full proportionate benefit of any decrease for the term of the contract. No price increases are to be billed to the State without prior written approval by the State Purchasing Bureau.

	Cost Proposal No Telephony Messaging	**Year One**	**Year Two**	**Year Three**
1	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 0 - 50,000 contacts	$0.45	$0.45	$0.45
2	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 50,001 - 75,000 contacts	$0.40	$0.40	$0.40
3	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 75,001 - 100,000 contacts	$0.35	$0.35	$0.35
4	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 100,001 - 250,000 contacts	$0.30	$0.30	$0.30
5	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 250,001 and up contacts	$0.25	$0.25	$0.25
6	GIS mapping fees if not included in base price add on per enrolled contact per year	N/A	N/A	N/A

Cost Proposal
Request for Proposal Number 6214 Z1

	Cost Proposal Including Telephony Messaging	Year One	Year Two	Year Three
7	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 0 - 50,000 contacts	$0.75	$0.75	$0.75
8	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 50,001 - 75,000 contacts	$0.70	$0.70	$0.70
9	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 75,001 - 100,000 contacts	$0.65	$0.65	$0.65
10	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 100,001 - 250,000 contacts	$0.60	$0.60	$0.60
11	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 250,001 and up contacts	$0.45	$0.45	$0.45
12	GIS mapping fees if not included in base price add on per enrolled contact per year	N/A	N/A	N/A

Note: Invoices are to be based on a monthly portion of the fixed annual cost per maximum enrolled contact of the billing month.
For example: if the State of Nebraska has 45,000 users on the 1st of the month, 48,000 on the 22nd of the month and 47,000 at the end of the month, the bidder will bill the state for 48,000 enrolled users for that month. If the annual cost is $1.20 and there are 48,000 enrolled users for that month, the bidder will bill the State of Nebraska for $0.10 (monthly rate) x 48,000 (enrolled users) = $4,800.00.

	Cost Proposal IPAWS	Year One	Year Two	Year Three
13	Software includes 95 individual IPAWS licenses to be accessed by NEMA, State Patrol and 93 counties.	$20,000	$20,000	$20,000

	Cost Proposal Custom Programming	Year One	Year Two	Year Three
14	Custom Programming at an hourly rate	$170	$170	$170

Cost Proposal
Request for Proposal Number 6214 Z1

	Cost Proposal Optional Products and Services	Year One	Year Two	Year Three
15	Rave Smartloader Automatic Data Loader per domain	$1,500	$1,500	$1,500
16	SMS Opt-in Keyword per keyword	$2,200	$2,200	$2,200
17	Rave Prepare per domain	$2,200	$2,200	$2,200
18	Enhanced RBAC per domain	$1,500	$1,500	$1,500

Cost Proposal
Request for Proposal Number 6214 Z1

OPTIONAL RENEWAL PERIODS

Price escalation of no more than 3% may be allowed for each renewal period.

	Cost Proposal – Optional Renewal Years No Telephony Messaging	Year Four Optional Renewal 1	Year Five Optional Renewal 2	Year Six Optional Renewal 3	Year Seven Optional Renewal 4	Year Eight Optional Renewal 5
1	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 0 - 50,000 contacts	$0.46	$0.48	$0.49	$0.51	$0.52
2	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 50,001 - 75,000 contacts	$0.41	$0.42	$0.43	$0.45	$0.46
3	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 75,001 - 100,000 contacts	$0.36	$0.37	$0.38	$0.39	$0.41
4	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 100,001 - 250,000 contacts	$0.31	$0.32	$0.33	$0.34	$0.35
5	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1.1, except Item 1a, unlimited use 250,001 and up contacts	$0.26	$0.27	$0.28	$0.29	$0.30
6	GIS mapping fees if not included in base price add on per enrolled contact per year	N/A	N/A	N/A	N/A	N/A

Cost Proposal
Request for Proposal Number 6214 Z1

	Cost Proposal - Optional Renewal Years Including Telephony Messaging	Year Four Optional Renewal 1	Year Five Optional Renewal 2	Year Six Optional Renewal 3	Year Seven Optional Renewal 4	Year Eight Optional Renewal 5
7	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 0 - 50,000 contacts	$0.77	$0.80	$0.82	$0.84	$0.87
8	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 50,001 - 75,000 contacts	$0.72	$0.74	$0.76	$0.79	$0.81
9	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 75,001 - 100,000 contacts	$0.67	$0.69	$0.71	$0.73	$0.75
10	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 100,001 - 250,000 contacts	$0.62	$0.64	$0.66	$0.68	$0.70
11	Per enrolled contact per year, Software as a Service, General Service Requirements Item 1, unlimited use 250,001 and up contacts	$0.46	$0.48	$0.49	$0.51	$0.52
12	GIS mapping fees if not included in base price add on per enrolled contact per year	N/A	N/A	N/A	N/A	N/A

	Cost Proposal – Optional Renewal Years IPAWS	Year Four Optional Renewal 1	Year Five Optional Renewal 2	Year Six Optional Renewal 3	Year Seven Optional Renewal 4	Year Eight Optional Renewal 5
13	Software includes 95 individual IPAWS licenses to be accessed by NEMA, State Patrol and 93 counties.	$20,600	$21,218	$21,854	$22,510	$23,185

	Cost Proposal – Optional Renewal Years Custom Programming	Year Four Optional Renewal 1	Year Five Optional Renewal 2	Year Six Optional Renewal 3	Year Seven Optional Renewal 4	Year Eight Optional Renewal 5
14	Custom Programming at an hourly rate	$175	$180	$185	$191	$197

Cost Proposal
Request for Proposal Number 6214 Z1

Cost Proposal – Optional Renewal Years Optional Products and Services		Year Four Optional Renewal 1	Year Five Optional Renewal 2	Year Six Optional Renewal 3	Year Seven Optional Renewal 4	Year Eight Optional Renewal 5
15	Rave Smartloader Automatic Data Loader per domain	$1,545	$1,591	$1,639	$1,688	$1,739
16	SMS Opt-in Keyword per keyword	$2,266	$2,334	$2,404	$2,476	$2,550
17	Rave Prepare per domain	$1,545	$1,591	$1,639	$1,688	$1,739
18	Enhanced RBAC per domain	$1,545	$1,591	$1,639	$1,688	$1,739

Rave Platform Architecture and Operational Security Overview

Platform Solutions:

Rave Alert™

Rave 911 Suite™

Rave Panic Button™

Rave Facility™

Rave Guardian™

Rave Prepare™

Rave Eyewitness™

Table of Contents

Table of Contents 2
Rave Platform Architecture 3
Data Centers & Network Configuration 4
Alert Messaging Infrastructure 6
Employee Screening and Security Training 7
Monitoring and Configuration 8
Encryption and Data Management 8
Business Continuity Plan and Incident Response 9
Privacy Policies and Data Protection 10
Security Audits 11
Safety Act Certification 12

Rave Platform Architecture

Rave Mobile Safety's public-safety grade infrastructure is architected for security, privacy protection, redundancy, and reliability. User interfaces in the products connect across secure connections to secure, distributed computing platforms with geographic redundancy and failover capabilities to provide a highly available, highly reliable platform that regularly services millions of transactions originating from mobile apps, web interfaces such as citizen and educational opt-in portals as well as from web interfaces to specific platform functionalities, messaging solutions, and lookups and real-time profile provisioning from inbound 9-1-1 volume via Smart911.

Application infrastructure is protected by firewalled security layers and network infrastructure, and transactions are captured, stored and analyzed on the platform through a variety of application layers detailed below.

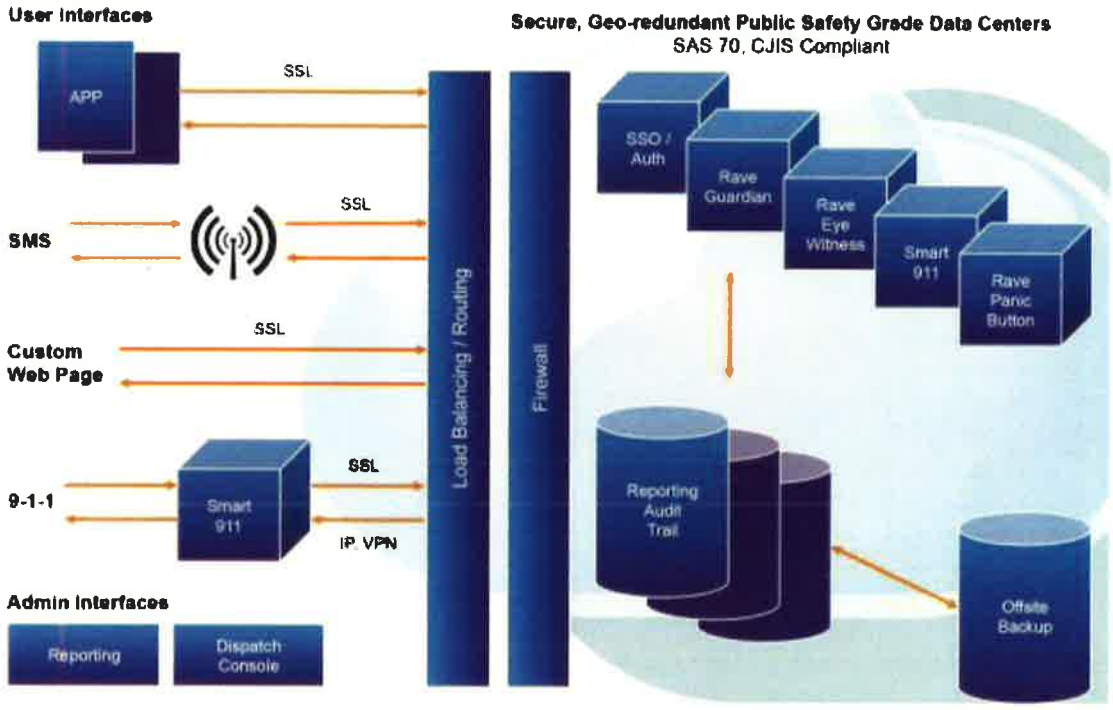


Figure 1: Rave Mobile Safety Platform Architecture overview.

Data Centers & Network Configuration

Rave's systems are built securely at all layers. We use the most up-to-date encryption, monitoring, and authentication technologies to protect your data in our databases and on our systems.

Rave Alert maintains 2 geo-redundant SAS-70, SOC II compliant, CJIS-compliant Tier 4 data centers, one in Massachusetts and one in California. We also support multiple geographically dispersed voice call centers. Our centers have redundant servers, power systems, and failover capabilities with one another. If a machine, power grid, or entire data center has an outage, the system automatically fails over to other resources. We replicate data between servers and centers, so no outage can cause a data loss.

These data centers make use of industry-standard safeguards such as 24/7 manned security, facility entry controlled by electronic keycards with pin codes, mantraps, and biometric scanners, locks on all cabinets, cages, and suites, and CCTV monitoring.

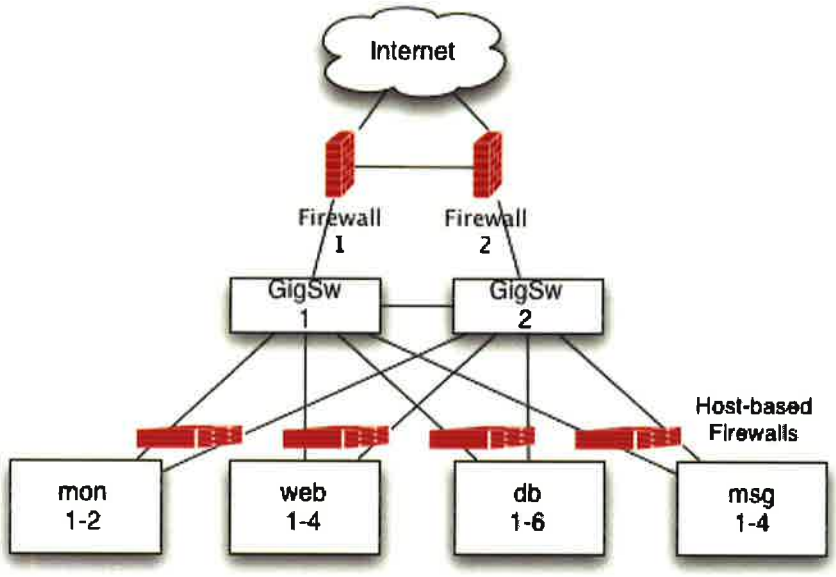
Physical access at each facility is controlled with three access safeguards. First, a named access control list identifies the only Rave representatives authorized to access the data center. At the data center, only these authorized personnel can pass the two-factor keycard and biometric control system. Finally, a combination lock secures the cabinets housing Rave's physical servers. This combination key is kept in an encrypted "password safe" only accessible to Rave System Administrators.

We monitor our servers 24x7 and provide all system maintenance to ensure Rave Alert is reliable, available, and provides high performance.

Configuration and Operational Security

Rave has constructed our system to only permit authorized access to customer data. Our production network, which contains customer data, is isolated from our corporate and development network. This means your data is never used in development testing or marketing materials. The production network itself is segmented by function, with separate segments for web activity, messaging, databases, and other functions. We monitor and tightly control network traffic between these segments, so customer data only moves when necessary for messaging and database maintenance. Each network tier is firewalled. These precautions allow us to confidently host your information, safe behind layers of network security.

An example of our network topology follows - each tier is firewalled as represented:



From a systems perspective, operational security measures include:

1. Monitoring and logging of all relevant system activity.

    a. Automated tools, both industry standard tools and bespoke security infrastructure, monitor logging in real-time.

2. Industry best practices for secure connectivity among all systems.

3. Untrusted certificates are not supported; trusted third-party certificates from known authorities accepted.

4. All interactions with systems are conducted over encrypted connections.

5. Public shared key encryption is enforced at all tiers where appropriate.

6. Access is limited to certified, trained personnel and tightly managed. Physical access to server environments is limited to specific individuals and regulated via biometric and other security measures. Physical security at each data center is controlled at each location through three sets of authentication:

    a. The first set is a named access control list, where only authorized representatives of Rave are listed.

    b. Second, there is a two-factor, key card and biometric control system that has only been authorized for the above-named personnel.

    c. Last, there is a combination key needed to unlock the cabinets housing Rave's physical servers. This combination key is kept in an encrypted "password safe" that

only Rave System Administrators have access to.

7. Data is hosted in a SAS-70 SOC Type II, Tier 4, CJIS-compliant co-location facility.
8. Offsite data backups are encrypted and stored in secure facilities.
9. Live customer data is never allowed in any test or QA environment.
10. All devices used to access the secure environment utilize required and up-to-date anti-virus and anti-penetration technologies. All employee disk drives are encrypted and audited for encryption via native device encryption.
11. Rave's Director of Operations oversees all auditing, with advice and best practices provided from ITCompass and other security consulting services and resources.
12. Rave Mobile Safety's Engineering and Technical Operations teams use several tools to consistently monitor the production servers, application, databases and mobile applications. Tools such as Ganglias and Nagios provide monitors at the server and OS level. Other tools like App Manager and DbTuna monitor application and database servers. Crashlytics is used to monitor mobile applications.

Alert Messaging Infrastructure

Messaging services are built for fault tolerance along multiple delivery paths, with each method supported in thread-safe concurrent processing with substantial redundancy.

There are no single points of failure within the Rave Alert system. Whereas all of our systems have been designed for high-availability, one area that is especially critical is the deliverability of emergency notifications. Our alerting infrastructure has been designed to tolerate failure at any point in the delivery chain with no message loss. If a process is interrupted anywhere in the chain, from computing a recipient list, to composing messages, to message delivery, the process will failover to another server and resume without loss or interruption. We make use of distributed transactions to handle maintaining state across our messaging server farm, and have multiple SMS connection binds and voice calling centers for message delivery.

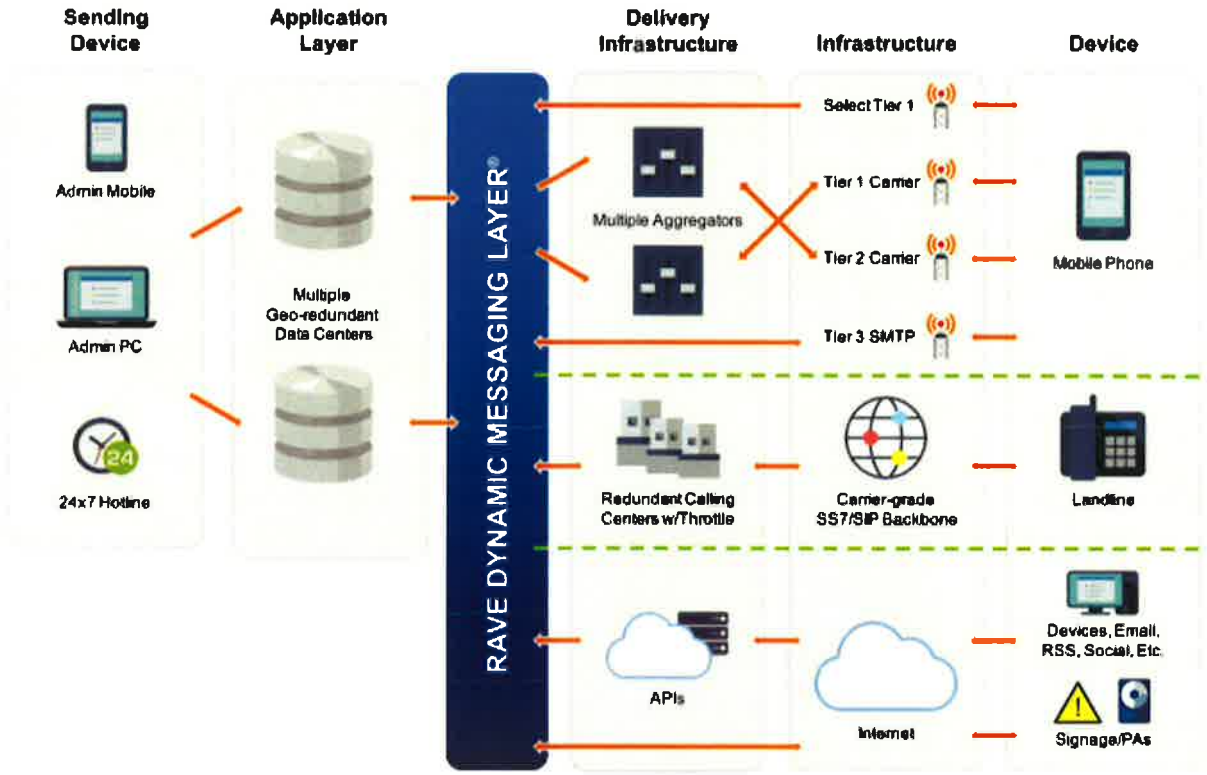


Figure 2: Rave Alert Infrastructure Overview

Because the SMS aggregation network in the U.S. has proven to be immature, our system is designed to support direct binds to leading carriers and supports multiple SMS aggregation firms such that we can fail over across them if one experiences reliability problems. This requires that we maintain multiple SMS short codes, and handle fail over and response reporting across multiple networks. We have made this investment in our infrastructure as we understand our customers' need to get their emergency messages delivered reliably 100% of the time.

Voice message delivery reliability is equally important. Rave's carrier-grade voice delivery architecture is able to deliver 30,000+ calls per minute from multiple geographically redundant calling centers, utilizing real-time congestion management to avoid overwhelming local exchanges. Each location's ARS (Automatic Route Selection) utilizes a minimum of six premier carrier route choices providing multiple streams.

Employee Screening and Security Training

Rave employees are screened via a third-party security firm as a condition of employment. Every member of Rave's staff undergoes best practice security awareness training provided by the same third-party security auditors described below. This training is updated on a regular basis and is mandatory for all employees.

In addition, Rave employees with permission to data center access and data management access are provided with additional training and tools to ensure the highest levels of safe handling and to guard against human and social engineering vulnerabilities.

Finally, Rave Services and Support staff maintain detailed policies and procedures to ensure against intrusions that may arrive via support channels, including social engineering. These policies are also tested, reviewed and hardened in Rave's auditing processes.

Monitoring and Configuration

Rave utilizes host-based, intrusion detection software to ensure that critical security and configuration files are not changed or Rave Technical Operations staff is notified immediately.

Rave also utilizes a configuration management system to ensure that all machines adhere to our corporate security policies. The configuration management system publishes policies such as authentication configuration, NTP/time, and syslog settings that help to ensure our systems are synchronized and our data is available.

Rave's Operations Team monitors numerous sources of information around potential vulnerabilities, and is granted authority to test and apply patches and protections for newly discovered vulnerabilities at its discretion. This policy is designed to ensure that vulnerabilities are addressed rapidly and effectively as new issues are identified and resolved across the technology industry.

Encryption and Data Management

All sensitive information is stored in encrypted format in the database. Rave uses the Java Cryptography Extensions (JCE), in conjunction with Sun's own cryptographic library to encrypt incoming customer data before storing. The JCE is a set of packages that provide a framework and implementations for encryption, key generation and key agreement algorithms.

Sensitive customer data is encrypted using the industrial strength TripleDES (112-bit) secret key algorithm. TripleDES is a minor variation to the Data Encryption Standard (DES), developed by an IBM team around 1974 and adopted as a national standard in 1977. As technology

advanced, DES proved vulnerable to brute-force attacks. Security professionals consider TripleDES to be roughly as secure as 128 bit ciphers such as AES and IDEA.

The disadvantage of secret key encryption is that the key must be kept secret from unauthorized users. To protect its keys, Rave uses secret key encryption in conjunction with a secure keystore that is accessible only by key system users.

Rave encrypts all transmission of sensitive data across public networks. Rave uses the latest 256-bit Secure Socket Layer technology for secure Internet Protocol transactions. All system requests over the Internet are encrypted over SSL.

Profile information is inaccessible on Rave's site to users outside the organization and guarded from external parties by both Rave's and the customer's optionally integrated directory services, secure authentication systems, and identity management systems. If a customer opts to manage authentication to the Rave system via LDAP, etc, authentication is performed by the customer -- meaning Rave's systems do not store user passwords. Rave maintains a strict privacy policy to protect user information.

Separate from our production sites, Rave also employs internal access control measures, including:

- Access to production systems and cryptographic keys and passwords are limited to key technology professionals via unique individual user ids and passwords.
- Production-level customer information is never accessible from any testing or development environments.
- Access to network resources and customer data is tracked and monitored.
- Passwords are changed on a regular basis and must conform to best practices for length and complexity.

Business Continuity Plan and Incident Response

For disaster recovery, Rave maintains failover capacity for our system, and keeps a business continuity plan to ensure infrastructure staff can communicate and strategize quickly when required. In the event of a catastrophic outage that completely took a collocation center offline, our Recovery Time Objective to be fully functional from our second collocation facility is 5 minutes. We routinely test our recovery plans by performing failovers between our colocation centers, with focus on specific tiers, hardware systems and subsystems, servers, and application infrastructure.

Rave maintains bespoke clustered, highly available, geo-redundant database server technology within its own infrastructures. At present, the system does not utilize cloud based storage providers for critical database or applications tiers.

Rave Mobile Safety's Technical and Operations Support teams are tasked with resolving any security issue or data breach, identifying the potential impact of the security issues, notifying any partners that may have been impacted, and performing post-issue analysis.

Rave's Operations, Engineering, Services, and Technical Support teams collaborate on response. Operations maintains responsibility for routine monitoring, site maintenance and uptime. Engineering is responsible for application integrity. Rave's Services and Technical Support teams provide the interface between the customer and internal operations.

Upon discovery of a critical issue, we would enact the following procedures:

1. **Initial notification** – Any customer who may have been impacted by the breach is notified. We then work with the customer on a notification plan for their messaging subscribers.
2. **Conduct an assessment** – Determine how the breach occurred and what data was compromised. A third party security firm may be utilized to assist in the assessment.
3. **Change passwords and audit access rights** – Change all system and administrator passwords, audit access rights to production environment including firewall rule base.
4. **Provide ongoing updates to customers** – Provide customers ongoing updates on the assessment and mediation until the issue has been addressed

Privacy Policies and Data Protection

Rave does not provide personally identifiable information in any way to telemarketers or other solicitors. This policy is clearly stated in both Rave's contract with the customer as well as Rave's privacy policy. Many Rave products, including most implementations of Rave Alert, do not capture or store data typically classified as PII in accepted industry definitions – for example, credit card information is never requested.

Client data is inaccessible on Rave's site to users outside of your authorized users and guarded from external parties by both Rave's and the client's secure authentication systems. If a client chooses to manage authentication to the Rave system via single sign-on options such as LDAP, Shibboleth, or SAML, the client's enterprise systems perform all authentication and enforce all authentication policies and password recovery measures -- meaning Rave's systems do not store user passwords at any persistence tier.

Rave designs our products to facilitate system security for our clients. Each product includes assignable access roles that allow you to ensure properly secure permissions within your organizations. Rave Mobile Safety has more than a decade of experience in the industry, allowing us to advise best-practices for large and diverse organizations to best structure their Rave systems to enhance and maintain system security. In addition, all system access sessions are captured in audit logs, allowing both clients and Rave to check access history should issues arise.

Rave's applications support strong authentication systems to prevent unauthorized logins and protect your authorized administrators' credentials. Each administrator uses a unique user-id for system access, and strong password requirements are enforced. Our authentication systems are routinely audited and refined. In addition, some products can integrate with single-sign-on mechanisms, further enhancing authorization security by storing passwords off the platform. Passwords and usernames, like all data in the Rave system, are encrypted to ensure secure logon for our clients. We encrypt passwords using multiple-iteration hashing with salting.

Public portals and voluntary opt-ins are managed according to industry best practices when appropriate, supporting a variety of mechanisms for maintaining subscription data and its privacy over time, designing for user friendly self-management of preferences, and maintaining accessibility and mobile-responsive operability in user interfaces.

Rave's privacy policies are clearly stated in both contractual vehicles as well as end user and customer-facing privacy policies. You can view a copy of our user-facing privacy policy here: https://getrave.com/help/Privacy.do.

Security Audits

To keep our security up to date, Rave's infrastructure, applications, and operations are annually audited by a third party, currently Compass ITC, a security firm specializing in vulnerability assessment. Reviews are comprehensive and include:

- Database account control and access
- Vulnerability of the web applications (40 penetration tests)
- Physical security and physical security policy
- Network security and network security policy
- Personnel security and personnel security policy
- Cryptography
- Firewall vulnerability and firewall rulebase audit
- OS security
- Backup and recovery process
- Intrusion detection system
- Wireless network security configuration

Compass ITC utilizes industry best practices and methodologies for penetration testing, such as the OWASP Guide/OWASP Top 10, Open Source Security Testing Methodology Manual (OSSTMM) and National Institute for Standards and Technology (NIST). Compass is also a SANS/GIAC Certified Web Application Penetration Tester. These methodologies and certificated training ensure a complete and consistent approach to the assessment.

All Compass ITC audits are reviewed internally at Rave via a formal process and improvements

to processes, procedures, and technology are scheduled and implemented based on the recommendations.

Safety Act Certification

Rave Mobile Safety is Safety Act certified by the U.S. Department of Homeland Security. For details on this certification, see http://www.safetyact.gov/.

Please Note: Details provided in this document are current at time of authoring and may be subject to change over time. This documents does not represent contractual commitments. Rave Mobile Safety's Services Levels Policy (SLP) and related contractual instruments govern all service commitments.

250 Williams Street | Suite E100 | Atlanta, GA 30303

INAP

January 3, 2019

Subject: SOC 2 Bridge Letter

Dear Valued Customer,

UHY LLP, Certified Public Accountants ("UHY") performed a SOC 2, Type II attestation engagement, examining the description by Internap Corporation ("INAP") of its Flagship Data Centers (as defined in the SOC 2 reports) and the suitability of the design and operating effectiveness of controls for the period from October 1, 2017 to September 30, 2018. UHY provided INAP reports dated December 20, 2018 which document the findings of UHY. These reports are available to our customers upon request.

This letter serves to provide assurance that since the examination was completed, INAP is not aware of any material changes in the controls reported, and all of INAP's reported procedures and controls are still in place and operating as documented in the SOC 2, Type II reports dated December 20, 2018.

The SOC 2, Type II report dated December 20, 2018 is a complete document and this letter is not designed, nor intended, to modify the report in any way. This letter is not intended to provide you a certification of the internal controls of INAP or suggest that INAP has performed any structured evaluation of its internal controls for the purpose of producing this letter. By providing this letter, we do not undertake to provide you with any updates or changes in the internal controls of INAP.

If you have any questions or if we can be of further assistance, please feel free to contact me at vmaxwell@inap.com, 404-865-7377, or contact your INAP representative.

Sincerely,

Vicki Maxwell

Vicki Maxwell
Director, Internal Audit
Internap Corporation

VPAT
Web Content Accessibility Guidelines 2.0 level AA

It is strongly recommended Technical Staff who are trained in Accessibility complete this form.

Accessibility points will be awarded based on: (1) the accuracy and detailed response to this form, and (2) how accessible your product is. Comments section must be filled in. NOTE: MN only adopted the standards that are level A and level AA. This list includes level AAA standards, which are optional and highlighted in yellow. Comments are not required for level AAA.

Principle 1: Perceivable – information and user interface components must be presentable to users in ways they can perceive.

Standard	Description	Apply Yes/No	Meets Yes/No	Comments (mandatory)
Guideline 1.1 Text Alternatives: Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.				
1.1.1	Non-text Content: All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below (Level A).	Yes	Yes	Rave Alert's text alternatives have been extensively tested to ensure they serve the equivalent purpose of our non-text content.
	• Controls, Input: If non-text content is a control or accepts user input, then it has a name that describes its purpose. (Refer to Guideline 4.1 for additional requirements for controls and content that accepts user input.)	• Yes	• Yes	• Rave Alert's non-text controls have descriptive names.
	• Time-Based Media: If non-text content is time-based media, then text alternatives at least provide descriptive identification of the non-text content. (Refer to Guideline 1.2 for the additional requirements for media.)	• Yes	• Yes	• Rave Alert time-based media all have appropriate text-based alternatives within the product. Very little use of time based media in use.
	• Test: If non-text content is a test or exercise that would be invalid if presented in text, then text alternatives at least provide descriptive identification of the non-text content.	• Yes	• Yes	• Rave Alert time-based media all have appropriate text-based alternatives within the product. Very little use of time based media in use.
	• Sensory: If non-text content is primarily intended to create a specific sensory experience, then text alternatives at least provide descriptive identification of the non-text content.	• No	• N/A	• Rave Alert does not contain any non-text content primarily intended to create a specific sensory experience.
	• CAPTCHA: If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided, and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities.	• Yes	• Yes	• Rave Alert complies with accessible CAPTCHA
	• Decorative, Formatting, Invisible: If non-text content is pure decoration, is used only for visual formatting, or is not presented to users, then it is implemented in a way that it can be ignored by assistive technology.	• Yes	• Yes	• Rave Alert complies.
Guideline 1.2 Time-based Media: Provide alternatives for time-based media.				

1.2.1	Audio-only and Video-only (Prerecorded): For prerecorded audio-only and prerecorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labeled as such (Level A): • Prerecorded Audio-only: An alternative for time-based media is provided that presents equivalent information for prerecorded audio-only content. • Prerecorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for prerecorded video-only content.	Yes • Yes • Yes	Yes • Yes • Yes	All content in video and multi-media training is also available through provided text manuals. • All content in video and multi-media training is also available through provided manuals • All content in video and multi-media training is also available through provided manuals
1.2.2	Captions (Prerecorded): Captions are provided for all prerecorded audio content in synchronized media, except when the media is a media alternative for text and is clearly labeled as such. (Level A)	No	N/A	All Rave Alert prerecorded audio content is a media alternative for text.
1.2.3	Audio Description or Media Alternative (Prerecorded): An alternative for time-based media or audio description of the prerecorded video content is provided for synchronized media, except when the media is a media alternative for text and is clearly labeled as such. (Level A)	No	N/A	All Rave Alert prerecorded audio content is a media alternative for text.
1.2.4	Captions (Live): Captions are provided for all live audio content in synchronized media. (Level AA)	Yes	No	Rave Alert does not provide captions for all live audio content. Our audio content is a media alternative to text content.
1.2.5	Audio Description (Prerecorded): Audio description is provided for all prerecorded video content in synchronized media. (Level AA)	Yes	Yes	Rave Alert's prerecorded video includes audio description.
1.2.6	Sign Language (Prerecorded): Sign language interpretation is provided for all prerecorded audio content in synchronized media. (Level AAA)	Yes	No	Rave Alert does not provide sign language interpretation for all prerecorded audio content. Our audio content is a media alternative to text content. Our videos show web interfaces that integrate with assistive technology, so our provided audio descriptions are embedded in the described interface.
1.2.7	Extended Audio Description (Prerecorded): Where pauses in foreground audio are insufficient to allow audio descriptions to convey the sense of the video, extended audio description is provided for all prerecorded video content in synchronized media. (Level AAA)	No	No	Rave Alert's included video content does not contain content where pauses in foreground audio are insufficient to allow audio descriptions. Our videos show web interfaces that integrate with assistive technology, so our provided audio descriptions are embedded in the described interface.
1.2.8	Media Alternative (Prerecorded): An alternative for time-based media is provided for all prerecorded synchronized media and for all prerecorded video-only media. (Level AAA)	Yes	Yes	All content in video and multi-media training is also available through provided manuals.
1.2.9	Audio-only (Live): An alternative for time-based media that presents equivalent information for live audio-only content is provided. (Level AAA)	Yes	No	Rave Alert does not provide an audio-only equivalent. All our time-based media content is available through audio description and provided manuals, in conjunction with an application that uses alt text and other settings compliant with assistive technology.
Guideline 1.3 Adaptable: Create content that can be presented in different ways (for example simpler layout) without losing information or structure.				
1.3.1	Info and Relationships: Information, structure, and relationships conveyed through presentation can be programmatically determined or are available in text. (Level A)	Yes	Yes	Rave Alert complies.

1.3.2	Meaningful Sequence: When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined. (Level A)	Yes	Yes	Rave Alert complies.
1.3.3	Sensory Characteristics: Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, size, visual location, orientation, or sound. (Level A)	Yes	Yes	Rave Alert complies.
Guideline 1.4 Distinguishable: Make it easier for users to see and hear content including separating foreground from background.				
1.4.1	Use of Color: Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. (Level A)	Yes	Yes	Where Rave Alert uses color coding, it is in conjunction with supporting text.
1.4.2	Audio Control: If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level. (Level A)	Yes	Yes	Rave Alert provides a pause-play button and volume control during review of voice messages.
1.4.3	Contrast (Minimum): The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: (Level AA) • Large Text: Large-scale text and images of large-scale text have a contrast ratio of at least 3:1; • Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. • Logotypes: Text that is part of a logo or brand name has no minimum contrast requirement.	Yes	Yes	Rave Alert complies.
1.4.4	Resize text: Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality. (Level AA)	Yes	Yes	Rave Alert complies.
1.4.5	Images of Text: If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text except for the following: (Level AA) • Customizable: The image of text can be visually customized to the user's requirements; • Essential: A particular presentation of text is essential to the information being conveyed.	Yes	Yes	Rave Alert complies. Text is used to convey information in this product, not images of text, with the exception of logos, which have alternate text. • Acknowledged • Acknowledged
1.4.6	Contrast (Enhanced): The visual presentation of text and images of text has a contrast ratio of at least 7:1, except for the following: (Level AAA) • Large Text: Large-scale text and images of large-scale text have a contrast ratio of at least 4.5:1; • Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. • Logotypes: Text that is part of a logo or brand name has no minimum contrast requirement.	Yes	Yes	Rave Alert complies. All images and text have a contrast ratio meeting AAA standards excluding the exceptions in this section. • Acknowledged • Acknowledged • Acknowledged
1.4.7	Low or No Background Audio: For prerecorded audio-only content that (1) contains primarily speech in the foreground, (2) is not an audio CAPTCHA or audio logo, and (3) is not vocalization intended to be primarily musical expression such as singing or rapping, at least one of the following is true: (Level AAA) • No Background: The audio does not contain background sounds. • Turn Off: The background sounds can be turned off. • 20 dB: The background sounds are at least 20 decibels lower than the foreground speech content, with the exception of occasional sounds that last for only one or two seconds.	No	N/A	Rave Alert does not contain prerecorded audio-only content. Users can record audio content through the product, which may record background noise depending on the user's location.

1.4.8	Visual Presentation: For the visual presentation of blocks of text, a mechanism is available to achieve the following: (Level AAA)	Yes	No	Rave Alert is compliant with Level AA WCAG guidelines for visual presentation, and some of the Level AAA guidelines in this question.
	• Foreground and background colors can be selected by the user.	• Yes	• No	• Rave Alert does not support color and contrast changes except as already provided in standard web browsers
	• Width is no more than 80 characters or glyphs (40 if CJK).	• Yes	• Yes	• Rave Alert complies by default.
	• Text is not justified (aligned to both the left and the right margins).	• Yes	• Yes	• Rave Alert complies by default.
	• Line spacing (leading) is at least space-and-a-half within paragraphs, and paragraph spacing is at least 1.5 times larger than the line spacing.	• Yes	• Yes	• Rave Alert complies.
	• Text can be resized without assistive technology up to 200 percent in a way that does not require the user to scroll horizontally to read a line of text on a full-screen window.	• Yes	• No	• Resizing Rave Alert requires horizontally scrolling to read text.
1.4.9	Images of Text (No Exception): Images of text are only used for pure decoration or where a particular presentation of text is essential to the information being conveyed. (Level AAA)	Yes	Yes	Rave Alert only uses images of text for logos.

Principle 2: Operable - User interface components and navigation must be operable.

Standard	Description	Apply Yes/No	Meets Yes/No	Comments
Guideline 2.1 Keyboard Accessible: Make all functionality available from a keyboard.				
2.1.1	Keyboard: All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints. (Level A)	Yes	Yes	All standard web functions are accessible via keyboard.
2.1.2	No Keyboard Trap: If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface, and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away. (Level A)	Yes	Yes	Rave Alert supports unmodified tab keys to navigate interfaces.
2.1.3	Keyboard (No Exception): All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes. (Level AAA)	Yes	Yes	All standard web functions are accessible via keyboard.

Guideline 2.2 Enough Time: Provide users enough time to read and use content.				
2.2.1	Timing Adjustable: For each time limit that is set by the content, at least one of the following is true: (Level A) • Turn off: The user is allowed to turn off the time limit before encountering it; or • Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or • Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the space bar"), and the user is allowed to extend the time limit at least ten times; or • Real-time Exception: The time limit is a required part of a real-time event (for example, an auction), and no alternative to the time limit is possible; or • Essential Exception: The time limit is essential and extending it would invalidate the activity; or • 20 Hour Exception: The time limit is longer than 20 hours.	No	N/A	Rave Alert does not include any time limits.
2.2.2	Pause, Stop, Hide: For moving, blinking, scrolling, or auto-updating information, all of the following are true: (Level A)	Yes	Yes	Rave Alert does not include any moving, blinking, or scrolling content. Our auto-updating information is not presented in parallel with other content, and takes the form of auto-updating text-based reports.
	• Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds, and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and	• No	• N/A	• Rave Alert does not include any moving, blinking, or scrolling components.
	• Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.	• No	• N/A	• Rave Alert's auto-updating content is not presented in parallel with other content.
2.2.3	No Timing: Timing is not an essential part of the event or activity presented by the content, except for non-interactive synchronized media and real-time events. (Level AAA)	Yes	Yes	Timing is not an essential part of the event or activity presented by Rave Alert's content.
2.2.4	Interruptions: Interruptions can be postponed or suppressed by the user, except interruptions involving an emergency. (Level AAA)	No	N/A	Rave Alert does not include interruptions.
2.2.5	Interruptions: Interruptions can be postponed or suppressed by the user, except interruptions involving an emergency. (Level AAA)	No	N/A	Rave Alert does not include interruptions.
Guideline 2.3 Seizures: Do not design content in a way that is known to cause seizures.				
2.3.1	Three Flashes or Below Threshold: Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds. (Level A)	Yes	Yes	Rave Alert does not contain anything that flashes.
2.3.2	Three Flashes: Web pages do not contain anything that flashes more than three times in any one second period. (Level AAA)	Yes	Yes	Rave Alert does not contain anything that flashes.
Guideline 2.4 Navigable: Provide ways to help users navigate, find content, and determine where they are.				
2.4.1	Bypass Blocks: A mechanism is available to bypass blocks of content that are repeated on multiple Web pages. (Level A)	Yes	Yes	Rave Alert complies. Some portions of the application permit users to skip repetitive navigation and others do not. As edits are made to the application support for skipping is added to that section.
2.4.2	Page Titled: Web pages have titles that describe topic or purpose. (Level A)	Yes	Yes	Rave Alert complies.

2.4.3	Focus Order: If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability. (Level A)	Yes	Yes	Rave Alert complies.
2.4.4	Link Purpose (In Context): The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general. (Level A)	Yes	Yes	Rave Alert complies.
2.4.5	Multiple Ways: More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process. (Level AA)	Yes	Yes	Rave Alert complies. Pages not steps in a process are reachable through several workflows.
2.4.6	Headings and Labels: Headings and labels describe topic or purpose. (Level AA)	Yes	Yes	Rave Alert complies.
2.4.7	Focus Visible: Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible. (Level AA)	Yes	Yes	Rave Alert supports standard browser functionality to display keyboard focus.
2.4.8	Location: Information about the user's location within a set of Web pages is available. (Level AAA)	Yes	Yes	Rave Alert includes indication of the user's location, and the current pages' relationship to the other pages around it.
2.4.9	Link Purpose (Link Only): A mechanism is available to allow the purpose of each link to be identified from link text alone, except where the purpose of the link would be ambiguous to users in general. (Level AAA)	Yes	Yes	Rave Alert's link text have been extensively tested to ensure link function is intuitive from link text.
2.4.10	Section Headings: Section headings are used to organize the content. (Level AAA)	Yes	Yes	Rave Alert complies.

Principle 3: Understandable - Information and the operation of user interface must be understandable.

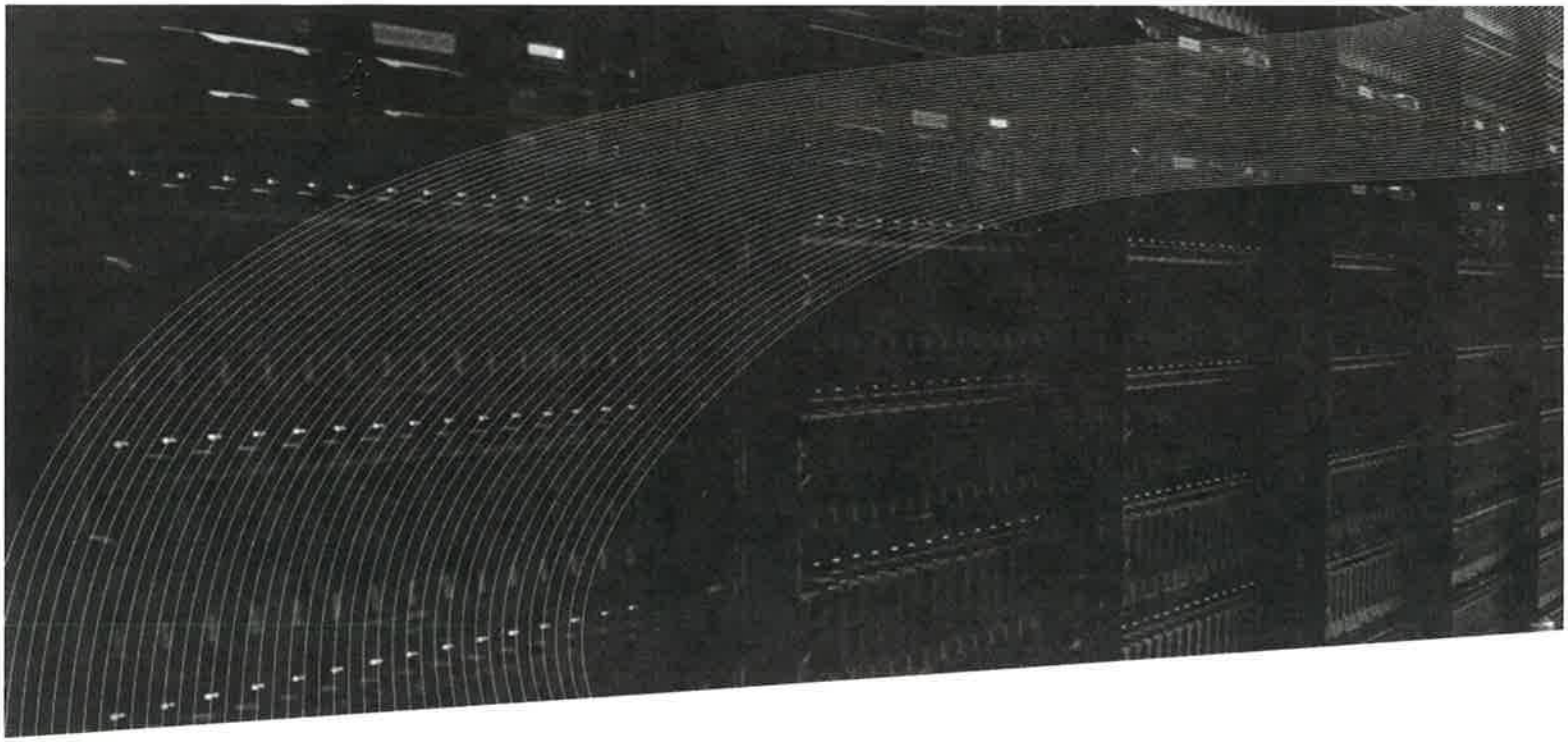
Standard	Description	Apply Yes/No	Meets Yes/No	Comments
Guideline 3.1 Readable: Make text content readable and understandable.				
3.1.1	Language of Page: The default human language of each Web page can be programmatically determined. (Level A)	Yes	Yes	Rave Alert complies.
3.1.2	Language of Parts: The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language, and words or phrases that have become part of the vernacular of the immediately surrounding text. (Level AA)	Yes	Yes	Rave Alert complies.
3.1.3	Unusual Words: A mechanism is available for identifying specific definitions of words or phrases used in an unusual or restricted way, including idioms and jargon. (Level AAA)	Yes	Yes	Rave Alert provides glossaries for words and phrases with product-specific meanings.
3.1.4	Abbreviations: A mechanism for identifying the expanded form or meaning of abbreviations is available. (Level AAA)	Yes	Yes	Rave Alert includes the extended form of abbreviations as appropriate.
3.1.5	Reading Level: When text requires reading ability more advanced than the lower secondary education level after removal of proper names and titles, supplemental content, or a version that does not require reading ability more advanced than the lower secondary education level, is available. (Level AAA)	No	N/A	Rave Alert is designed to not require advanced reading ability.
3.1.6	Pronunciation: A mechanism is available for identifying specific pronunciation of words where meaning of the words, in context, is ambiguous without knowing the pronunciation. (Level AAA)	No	N/A	Rave Alert does not contain words where meaning is ambiguous without pronunciation.
Guideline 3.2 Predictable: Make Web pages appear and operate in predictable ways.				
3.2.1	On Focus: When any component receives focus, it does not initiate a change of context. (Level A)	Yes	Yes	Rave Alert complies.
3.2.2	On Input: Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behavior before using the component. (Level A)	Yes	Yes	Rave Alert complies.

3.2.3	Consistent Navigation: Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user. (Level AA)	Yes	Yes	Rave Alert complies.
3.2.4	Consistent Identification: Components that have the same functionality within a set of Web pages are identified consistently. (Level AA)	Yes	Yes	Rave Alert complies.
3.2.5	Change on Request: Changes of context are initiated only by user request or a mechanism is available to turn off such changes. (Level AAA)	Yes	Yes	Rave Alert initiates changes of context by user request.
Guideline 3.3 Input Assistance: Help users avoid and correct mistakes.				
3.3.1	Error Identification: If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text. (Level A)	Yes	Yes	Rave Alert complies.
3.3.2	Labels or Instructions: Labels or instructions are provided when content requires user input. (Level A)	Yes	Yes	Rave Alert complies.
3.3.3	Error Suggestion: If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content. (Level AA)	Yes	Yes	Rave Alert specifies required error response actions where appropriate.
3.3.4	Error Prevention (Legal, Financial, Data): For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: (Level AA) • Reversible: Submissions are reversible. • Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. • Confirmed: A mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.	Yes • Yes • Yes • Yes	Yes • Yes • Yes • Yes	Two of the following traits are true for Rave Alert. Data is checked for input errors and users have an opportunity to correct them, and the product confirms inputted data and provides a dedicated page for users to review, confirm, and correct information prior to final submission. • Rave Alert complies, where appropriate. • Rave Alert complies. • Rave Alert complies.
3.3.5	Help: Context-sensitive help is available. (Level AAA)	Yes	Yes	Rave Alert complies.
3.3.6	Error Prevention (All): For Web pages that require the user to submit information, at least one of the following is true: (Level AAA) • Reversible: Submissions are reversible. • Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. • Confirmed: A mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.	Yes • Yes • Yes • Yes	Yes • Yes • Yes • Yes	Two of the following traits are true for Rave Alert. Data is checked for input errors and users have an opportunity to correct them, and the product confirms inputted data and provides a dedicated page for users to review, confirm, and correct information prior to final submission.

Principle 4: Robust - Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.

Standard	Description	Apply Yes/No	Meets Yes/No	Comments
Guideline 4.1 Compatible: Maximize compatibility with current and future user agents, including assistive technologies.				
4.1.1	Parsing: In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features. (Level A)	Yes	Yes	Rave Alert complies.

4.1.2	Name, Role, Value: For all user interface components (including but not limited to: form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies. (Level A)	Yes	Yes	Rave Alert complies.



INDEPENDENT SERVICE AUDITOR'S REPORT

INAP CORPORATION – Santa Clara, CA (SJE011)

Flagship Data Center Services

Report on Controls at a Service Organization

Relevant to Security and Availability
(SOC 2 Type 2)

For the Period
October 1, 2017 – September 30, 2018

UHY LLP
Certified Public Accountants

Confidential – Limited Distribution Authorized
by INAP

INAP™

INAP CORPORATION

Report on Controls at a Service Organization Relevant to Security and Availability (SOC 2 Type 2)

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT 3

II. MANAGEMENT'S ASSERTION 4

III. DESCRIPTION OF THE INAP CORPORATION SYSTEM – 2151 Mission College Boulevard, Santa Clara, CA 95054 (SJE011) DATA CENTER SERVICES 5

- Company Background and Service Offerings 5
- The Aspects of the System and a Description of its Boundaries 5
- Risk Assessment 6
- Information and Communication Systems 6
- Monitoring 7
- Control Environment and Policy and Procedural Components 7
- Infrastructure, Environmental, and System Monitoring Components 8
- Personnel, Security, and Software System Components 9
- Data Used and Supported by the System 14
- Complementary User Entity Control Considerations 15

IV. INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITORS 17

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors of INAP Corporation:

Scope

We have examined INAP Corporation's accompanying description of its SJE011 Flagship Data Center Services system found in Section 3 titled "Description Of The INAP Corporation System – Santa Clara (SJE011) Data Center Services" throughout the period October 1, 2017 to September 30, 2018 (description) based on the criteria for a description of a service organization's system set forth in DC 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that INAP Corporation's service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability (applicable trust services criteria) set forth in TSP 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at INAP Corporation, to achieve INAP Corporation's service commitments and system requirements based on the applicable trust services criteria. The description presents INAP Corporation's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of INAP Corporation's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

INAP Corporation is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that INAP Corporation's service commitments and system requirements were achieved. In Section 2, INAP Corporation has provided the accompanying assertion titled "Management's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. INAP Corporation is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A member of UHY International
a network of independent accounting and consulting firms

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Information Provided By The Independent Service Auditors" of this report.

Opinion

In our opinion, in all material respects—

a. the description presents INAP Corporation's SJE011 Flagship Colocation Data Center system that was designed and implemented throughout the period October 1, 2017 to September 30, 2018 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2017 to September 30, 2018 to provide reasonable assurance that INAP Corporation's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if user entities applied the complementary user entity controls assumed in the design of INAP Corporation's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2017 to September 30, 2018 to provide reasonable assurance that INAP Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary user entity controls assumed in the design of INAP Corporation's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of INAP Corporation, user entities of INAP Corporation's SJE011 Flagship Colocation Data Center system during some or all of the period October 1, 2017 to September 31, 2018, business partners of INAP Corporation subject to risks arising from interactions with the INAP Corporation system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is intended solely for the information and use of management of the service organization and other specified parties. This report is not intended to be, and should not be, used by anyone other than the specified parties.

UHY LLP

Atlanta, GA
December 20, 2018

II. MANAGEMENT'S ASSERTION

Assertion of the Management of INAP:

We have prepared the accompanying description of INAP's SJE011 Flagship Data Center Services system titled "Description Of The INAP Corporation System – Santa Clara, CA (SJE011) Data Center Services" throughout the period October 1, 2017 to September 30, 2018 (description) based on the criteria for a description of a service organization's system set forth in DC 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*] (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the SJE011 Flagship Data Center Services system that may be useful when assessing the risks arising from interactions with INAP's system, particularly information about system controls that INAP has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at INAP Corporation, to achieve INAP Corporation's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

1) The description presents INAP's SJE011 Flagship Data Center Services system that was designed and implemented throughout the period October 1, 2017 to September 30, 2018 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period October 1, 2017 to September 30, 2018 to provide reasonable assurance that INAP Corporation's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of INAP Corporation's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period October 1, 2017 to September 30, 2018 to provide reasonable assurance that INAP Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of INAP Corporation's controls operated effectively throughout that period.

Signature: John Filipowicz

Title: SVP, CIO

III. DESCRIPTION OF THE INAP CORPORATION SYSTEM – 2151 Mission College Boulevard, Santa Clara, CA 95054 (SJE011) DATA CENTER SERVICES

Company Background and Service Offerings

INAP is the high-performance Internet infrastructure provider that powers the applications shaping the way we live, work, and play. INAP's hybrid infrastructure delivers performance without compromise – blending virtual and bare-metal cloud, hosting, and colocation services across a global network of data centers, optimized from the application to the end user and backed by rock-solid customer support and a 100% uptime guarantee. Since 1996, companies have relied on INAP to make their applications faster and more scalable.

INAP operates in two business segments: Data Center and Network Services, which includes Colocation and IP services, and Hosting Services. The scope of this report focuses on data center services, which primarily include physical space for collocating customers' network and other equipment plus associated services such as redundant power, environmental controls, and security.

INAP uses a combination of facilities that are operated by INAP and by third parties, referred to as INAP datacenters and non-core sites, respectively. INAP charge monthly fees for data center services based on the amount of square footage and power that a customer uses. This report is related to the Santa Clara (SJE011) INAP datacenter.

The Aspects of the System and a Description of its Boundaries

INAP is primarily responsible for the following types of activities related to data center services at the 2151 Mission College Boulevard, Santa Clara, CA 95054 (SJE011) INAP datacenter:

- Providing a safe, secure facility for customers. Related security requirements are supported by badge access systems, video surveillance cameras, and on-site 24 / 7 / 365 manned security and controls designed to ensure that only authorized individuals have access to the facility.
- Ensuring that networks and systems are available for use by customers, as defined by service level agreements (SLAs) agreed to in advance with the customer. Availability requirements are supported by an environmentally stable facility with uninterruptable power for the customers. Environmental controls and redundancy features must be periodically serviced and maintained to ensure effective operation.
- Resolving customer complaints, issues, and incidents on an as needed basis, or providing administrative services that customers require to maintain the availability and related security of their systems.
- Consistently applying an infrastructure change management process designed to ensure that only authorized, adequately planned, and supervised changes to the facility are performed.

INAP provides the following customer support services, which enhance the security and availability of the system by communicating related issues and requests with the customer. These services are primarily carried out by Network Operations Center (NOC) personnel.

- Responding to requests for support services.

- Responding to requests for changes (additions, modifications, and removals) to the customer's list of designated contacts. Requests for changes to customer contacts that have physical access are handled using this process.
- Responding to, and escalating, customer complaints and issues regarding the availability and / or related security of their services.
- Communicating changes, issues, and incidents to customers that have the potential to affect them.

INAP is not responsible for providing the following services for its colocation customers, unless these services are agreed to in advance under INAP's other service offerings (IP services, cloud services, hosting services, or hybridized services), which are not included within the scope of this report. Customers are responsible for performing these functions.

- Applying logical access security controls, including user authentication, password complexity requirements, password history requirements, password change procedures, account lockout procedures, and related procedures.
- Protecting and maintaining the network security of system resources (for example, secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services).
- Maintaining system components and configurations, including the application of change controls and procedures as necessary.
- Data encryption controls and the secure transfer of data through networks, including public, semi-private, and virtual private networks.
- Performing data backup procedures and data classification procedures as necessary.
- Protecting systems against infection by computer viruses, malicious codes, and unauthorized software.

Customers may choose to have INAP perform certain of these functions through INAP's other service offerings, which are not included within the scope of this report.

Risk Assessment

INAP uses various methods to manage risks that could impact the Company's ability to deliver service to customers. Management also assesses risks that inherently arise from the expansion of the business, whether organically or inorganically. This may include managing risks that are rooted in changes in personnel, technology, or the Company's operating environment. Additionally, management engages third parties to periodically assess risks to the achievement of security and availability objectives. Management revisits these assessments annually to ensure these risks are appropriately mitigated. Lastly, management performs an annual companywide risk assessment, which includes INAP datacenters.

Information and Communication Systems

INAP's management team is responsible for the detailed design and effective operation of the Company's internal controls. As part of this process, management communicates responsibilities and expectations to company personnel through both formal and informal means. Internal controls are evaluated by Internal Audit throughout the year as part of its internal audit reviews. Testing results and exceptions identified

during the audits are reported to management on a consistent basis. Management ensures that any internal control deficiencies identified are addressed and communicates expected timelines for doing so.

Monitoring

INAP's management team, including support from its Internal Audit department, continuously monitors the effectiveness of the Company's system of internal controls through the performance of periodic and annual audits of internal controls. Any deficiencies in the Company's system of internal controls are reported to management, assessed, and addressed. Management's consistent oversight of internal controls helps the Company identify deficiencies in the system, ensuring the adequacy of the process. Additionally, management has implemented security and availability monitoring controls in the form of periodic external inspections, metrics reviews, and incident monitoring.

Control Environment and Policy and Procedural Components

INAP data center operational policies and procedures are documented in various ways and are readily available to employees and customers. The responsibility and accountability for developing and maintaining these polices, and changes and updates to these policies, are assigned to the appropriate data center employees. Additionally, the information in these policies is reviewed on an annual basis by appropriate data center employees.

Each INAP data center has a specific Data Center Operations Manual kept in a binder and physically available for employees in case of an emergency. The Data Center Operations Manual is reviewed and approved by Data Center Operations management on an annual basis to ensure the information is up-to-date and accurate.

The Network Operations Center (NOC) uses its own intranet webpage dedicated to its policies and procedures. Content is updated in real time on the intranet webpage to ensure NOC employees are always aware of the newest policy or procedures. On an annual basis, NOC management performs a review of information on the NOC intranet webpage to ensure the information is up-to-date and accurate. The NOC uses a ticketing system to track all incidents and customer requests. Incidents are escalated as necessary and tracked until resolution.

Each customer in INAP data centers is given a New Customer Guide, Customer Service Manual, and Service Level Agreement (SLA). These documents include all necessary customer facing information and procedures to follow for many common questions / requests, such as system availability issues and what to do when a possible security breach is identified, along with many other incident responses. The information in the Customer Service Manual is reviewed on an annual basis by business unit management to ensure the information is up-to-date and accurate. Additionally, INAP customers connect to INAP via the INAP website and online customer portal. INAP's website hosts a detailed description of the data center services and the portal houses customer specific information and enables customers to contact INAP directly through the system. This customer portal, along with ad hoc communication methods are used to ensure transparent communication with customers.

The description of INAP data center operations can be broken down into the specific components of Infrastructure, Software, People, and Procedures.

Infrastructure, Environmental, and System Monitoring Components

INAP's data center operations consist of a strong physical infrastructure, including secure facilities featuring N+1 redundancy for both power and cooling, along with fire protection and system monitoring. The existing facility and environmental standards at the data centers are designed to ensure that uptime is maximized by providing redundancy to key facility and environmental systems.

Monitoring Environmental Conditions and Critical Work Authorizations

Data center environmental conditions are constantly monitored and reported via an automated Building Management System (BMS). Data center technicians and INAP's centralized Network Operations Center (NOC) personnel monitor a BMS console which reports the real-time status of power, HVAC, temperature, and fire detection / suppression conditions. If any issues or incidents with these environmental systems arise, the console displays an alert and e-mails data center personnel.

INAP has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations/modifications are documented and authorized to assure minimal impact to the customers. Periodically, the Company obtains the services of a third-party data center risk assessment expert to identify potential threats of disruption. These results are revisited annually by INAP data center and operations management to assess the risk associated with the threats identified.

Smoke / Fire Detection

The smoke / fire detection system in the data centers is comprised of smoke detectors and either a particulate sampling system or a very early smoke detection apparatus (VESDA) system that detects smoke during the very early stages of combustion. The smoke detection system is the first line of defense against fire in the facility. When smoke is detected by the system, an alarm is generated in the facility control room, and the BMS generates e-mail alerts to data center employees.

The smoke detection system is inspected and serviced at least annually to ensure effective operation.

Fire Suppression

The fire suppression system consists of a pre-action dry pipe system. The pre-action dry pipe system is designed to keep water out of the sprinkler system plumbing in the data center areas during normal operations. If smoke and / or excessive heat is detected, and a sprinkler fusible head melts as a result, water is pumped into the sprinkler systems for the affected zone(s) only. The BMS continuously monitors and reports the status of the fire suppression system.

The fire suppression systems are inspected and serviced at least annually to ensure effective operation.

Clean agent fire extinguishers are also provided throughout the data center for accessibility in the event of a fire within the data center (or elsewhere in the building).

Fire extinguishers are inspected and serviced at least annually to ensure effective operation.

Heating, Ventilation, and Air Conditioning (HVAC)

Multiple HVAC units control both temperature and humidity within the data center and are configured in a redundant formation to ensure operation continues if a unit fails. Temperature and humidity are maintained to current SLA standards. The HVAC units are monitored by the BMS within the facility control room and NOC.

HVAC units are inspected and serviced at least annually to ensure effective operation.

Utility Power and Backup Power Systems

Data center power is provided by feeds from the local utility provider to support daily operations. The power is channeled into an uninterruptible power supply (UPS) system, which conditions the power to be supplied to data center equipment. The UPS system allows for customers to opt for redundant N+1 power feeds to their equipment. In the event of a utility power outage, the UPS system seamlessly draws backup power from a battery farm which will supply power for 15 to 20 minutes until diesel generators power up. INAP maintains a sufficient on-site fuel reserve, which gives the backup generators capability to power the data center for at least 48 hours.

Each of INAP's datacenters maintain contracts with fuel companies for the delivery of fuel as needed.

The UPS systems and generators are inspected and serviced at least annually to ensure effective operation. The operating effectiveness of backup power systems are confirmed at least annually, through load bank testing and / or other methods.

Personnel, Security, and Software System Components

INAP's commitment to competence includes management's determination of the levels of competence and expertise required for each position at the data center, ensuring highly technical and customer service focused data center employees. INAP provides 24 / 7 manned facilities with a host of security features designed to protect the customer's equipment and network connectivity. INAP controls ingress and egress using electronic keycard and / or biometric software. All cages and cabinets are securely locked and Closed-Circuit Television (CCTV) cameras monitor and record activity within each facility.

Organizational Structure and Assignment of Authority and Responsibility

INAP has developed an organizational structure that adequately suits the nature and scope of its operations. The Company has developed organizational charts that internally convey employee reporting relationships, operational responsibilities, and the overall organizational hierarchy.

Human Resource Policies and Practices

INAP's human resource department has policies and established practices that govern the hiring, termination, evaluation, promotion, counseling, and compensation of current and prospective company employees. A documented set of human resource, operational, and financial policies and procedures, along with a complete list of internal controls are made available to applicable employees via the intranet. The Company has a written Code of Conduct that is communicated to and certified by all employees annually. The Code details the company's expectations regarding behavior, ethics, and business practices that every employee must abide by.

Detailed job descriptions and organizational charts convey the requirements for each position. INAP also facilitates employee development through annual evaluations, on-site training, and the allocation of funds for other relevant training. New hire policies include the requirement that background checks be performed on all new employees prior to commencing employment with INAP. Newly hired data center employees receive training and are made aware of customer facing documents and other internal policies covering system security and availability. For terminated employees, INAP has a formal process for decommissioning access to company records and systems in a timely manner.

Security Staff

A contracted security company employs and provides INAP's data center security resources. Such outsourcing ensures consistency of training, performance, metrics, and supervision. Responsibilities of security include, but are not limited to the following.

- Monitoring of Physical Security Systems
- Loss Prevention
- Internal Investigations
- Security Policies and Procedures Compliance

Security Control

All INAP data centers have Security and INAP Data Center technicians to control access, monitor security alarms, monitor CCTV camera surveillance, and support security-related operational activities 24 / 7 / 365. Security personnel or INAP on-duty engineers are on-site 24 hours a day, 7 days a week, 365 days a year. The Security Control Desk performs the following.

- Real-time monitoring of data center door alarms
- Real-time monitoring of data center CCTV cameras
- Centralized security service and emergency dispatch communications for Security Staff, as well as for local fire departments, police departments, and other emergency response resources
- Electrical power support for continuous operation of communications, lighting, CCTV, intrusion detection, and alarm monitoring equipment in the event of utility power loss

INAP on-duty engineer monitors security alarms, CCTV camera surveillance, and support security-related operational activities remotely 24 / 7 / 365. INAP on duty engineer remotely performs the following:

- Real-time monitoring of data center door alarms
- Real-time monitoring of data center CCTV cameras

Surveillance and Monitoring

INAP data centers employ a CCTV system to record and facilitate monitoring of the data center. Cameras are positioned to provide views of critical areas, including perimeter doors, main entrances and exits, shipping & receiving, and other areas of importance.

INAP security desk personnel monitor the signals from the CCTV system. The desk is connected by secure cables to the cameras throughout the facility to permit both interior and exterior surveillance.

Cameras are recorded on site via digital video recorders 24 / 7 / 365. These visual records are retained for at least 90 days to provide details of activity at INAP data centers. INAP provides dedicated 24 / 7 / 365 continuous power supply (CPS) and standby emergency power via generator to support security systems.

Access Control

INAP employs a computerized Access Control System (ACS) to control physical access to the data centers. The ACS utilizes proximity card readers with pin codes or biometrics to control access into the data center floor, perimeter doors, shipping & receiving areas, storerooms, and other critical areas. Customers and employees (including contractors and security guards) must follow formal access request and approval processes before physical access to the data centers is granted. Additional access control features are as follows.

- Access to the data center and other restricted areas is specifically limited to authorized individuals.
- INAP access badges and / or biometrics are required to gain entry to critical areas.
- Customers, Vendors, Contractors, Visitors and non-data center employees must sign in at the security desk prior to entry into the data center. INAP personnel verifies log accuracy and reconciles log with ACS.
- Customers, Vendors, Contractors, and other Visitors must be sponsored by an INAP-approved host to gain access if not on the Customer-Approved List.
- All Customers, Vendors, Contractors, and Visitors on the Customer-Approved List must check in with the Security Desk upon arrival with photo identification if they require the physical key to access cages. Those customers with badge cage access will have automatic access to their cages.
- Visitors and others not on the Customer-Approved List are escorted while in the data center and other critical areas.
- Guest access for approved Contractors is generally limited to particular areas where work is being performed. Long term contractors are granted more general access via personal badges.
- Employees with access to the data center are limited to those with a specific business need or job function.

Administrator access (add, modify and delete users) in the ACS is restricted to appropriate personnel based on job roles and responsibilities and reviewed during periodic access reviews. Data Center Management authorizes Administrator access to the keycard system based on the individual's job responsibilities.

The ACS is also used to monitor, notify, and log security alarms. The system monitors the following.

- Perimeter / external doors
- Restricted area doors
- Data center doors
- Shipping / receiving doors

The system is programmed to log all card reader activity. It also generates alarms for forced doors, propped doors, and denied card read attempts.

Visitor / Sales Tour Access

All INAP data center tours must be coordinated with an INAP representative. Tours of the data center and other restricted areas require an escort from an authorized INAP employee.

Customer Access

Each customer is permitted to designate individuals with access to INAP data centers via the Network Operations Center (NOC). The customers make requests for access through the NOC via email, phone call, or the online Customer Portal. The NOC manages customers' respective Customer Access Lists (CALs) within the Ubersmith Facility Management application. Update access to the CAL is reviewed for appropriateness based on job responsibilities on an annual basis. Data center security has view access to the CALs and will only allow individuals listed on a Company's CAL access to the data center. The customer is responsible for requesting additions, modifications, or deletions to access; the NOC is responsible for management of the Customer Access List. Upon notification of a customer employee termination or revocation of customer agreement, physical access to the data center is revoked. Customers are responsible for retaining a terminated employee's access badge and either destroying it or returning it to INAP security.

Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment.

Cages are secured via one of two possible means: Physical key or electronic badge reader.

1. Physical key - Keys are maintained by INAP security personnel or INAP onsite engineer. After the security personnel or INAP onsite engineer determine appropriate authority per the CAL, they escort the customer to the cage and unlock it for them; or

2. Badge reader access - access is controlled via the ACS, similar to that of data center access.

Cabinets are secured via one of two possible means: Physical key or combination lock.

1. Physical key - Keys are maintained by INAP security personnel and INAP onsite engineer. After the security personnel or INAP onsite engineer determine appropriate authority per the CAL, they escort the customer to the cabinet and unlock it for them; or

2. Combination lock - access is controlled via the use of a customer specific combination code.

Customers are responsible for ensuring their cage and cabinet(s) are properly locked before leaving the facility.

Employee and Security Guard Access to Data Center

Access to the data center is restricted to only those INAP employees with a legitimate business need. Access, if temporarily required for other employees whose job functions do not necessitate access to the data center on a day-to-day basis, is granted on a case-by-case basis by the data center manager, and these employees must be escorted by data center personnel. Physical access to the data center is revoked upon termination of INAP employees and security guards.

Contractor and Vendor Access to Data Center

Access to the data center is restricted to Contractors and Vendors with a legitimate business purpose. Access is granted with a daily temporary badge and logged with security unless the Contractor or Vendor will be on site for an extended period of time or multiple times over an extended period (i.e., multiple weeks). Data Center management will notify Security of an expected Contractor or Vendor, and if a Contractor or Vendor arrives unexpectedly, Security will contact Data Center management to gain approval for temporary access. Temporary access cards are returned to security prior to leaving the facilities. If a temporary badge is not returned at the end of the day, it is disabled in the system by Security. Physical access to the data center is revoked upon completion of the contractors' and / or vendors' duties.

General Visitor Rules

- All visitors must be escorted at all times by an authorized host or employee.
- INAP data center regulations must be strictly followed at all times. Any individual (including INAP employees) not adhering to these rules will be escorted from the data center by staff and / or security.
- Badges must be displayed at all times within the facility.

Customer and Employee Access Review

INAP data center personnel perform audits to validate the appropriateness of access permissions in the Access Control System (ACS). The following audits are performed quarterly by Data Center Operations management.

1. Customer Access permissions in the ACS are validated against the Ubersmith Facilities Access list.
2. Employee, Contractor, and Security Guard access in the ACS are reviewed for appropriateness.
3. Employees with access to add, modify, and delete users in the ACS are reviewed for appropriateness.

Logical and Network Protections for the Access Control System

Access to the keycard system is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.

Password length and complexity requirements are established for the INAP internal network. Password settings for the keycard system are the same as for the internal network since the system uses single sign on.

Anti-virus software for network workstations and keycard system servers is installed and operating effectively. The Company has firewalls in place to limit access over the internet to the central keycard system application and database. Connections via VPN tunnel between the central physical access systems and each data center are protected using encryption.

Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the appropriate business unit representative for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.

Logical and Network Protections for the Ubersmith Facility Management Application

Access to the Ubersmith application is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.

Password settings for the Ubersmith application include length and change requirements. Account lockout features are set to lock out or disable a user after a number of failed login attempts to the Ubersmith application.

Connections to the Ubersmith application via the internet are protected using encryption.

Data Used and Supported by the System

Client Data

INAP does not manage client data or content. Clients are responsible for applying logical access security controls, network security controls, data encryption controls, and related procedures to protect their data, as well as performing data backup procedures and data classification procedures as necessary.

Data Managed by INAP

Listing of Customer Contacts – INAP maintains a listing of all customer contacts with approved access to the data center. The listing provides the privileges granted to each contact, including whether or not they have physical access, may request tech support, or add other contacts to the approved listing managed by INAP. Customers may request a report listing all individuals on this approved listing, as well as their privileges.

Physical Access Control System Lists and Customer, Employee, Security Guard, and Contractor Key Badges – INAP maintains a listing of all individuals with physical access to the data center. This is managed using the Access Control System. Customers may request a report listing all individuals who have physical access to their cage or cabinet.

Physical Access Activity Logs – The Access Control System maintains records of all physical access attempts to the data center (both successful and unsuccessful). Temporary visitor and contractor logs are maintained by the Security Desk.

Complementary User Entity Control Considerations

INAP systems were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specified internal controls at user organizations is necessary to achieve certain control objectives included in this report. INAP has considered the following user entity control considerations in developing the controls which are described in Section III of this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at INAP. User auditors should consider whether the following controls have been placed in operation at user organizations. This is not a comprehensive list of all controls that should be employed at user organizations.

- User organizations are responsible for understanding and complying with their contractual obligations. (all criteria)
- User organizations are responsible for ensuring the supervision, management, and control of the use of INAP's services by their personnel. (all criteria)
- User organizations are responsible for designating authorized individuals for access requests to INAP's data center. (criteria CC5.4, CC5.5)
- User organizations are responsible for notifying INAP of terminated employees. (criteria CC5.4, CC5.5)
- User organizations are responsible for retaining a terminated employee's access badge and either destroying it or returning it to INAP security. (criteria CC5.4, CC5.5)
- User organizations are responsible for changing their cabinet combination lock password after individuals with knowledge of the current combination are terminated. (criteria CC5.4, CC5.5)
- User organizations are responsible for periodically reviewing their Customer Access Lists. (criteria CC5.4, CC5.5)
- User organizations are responsible for immediately notifying INAP of any actual or suspected information security breaches, including compromised user accounts. (criteria CC6.2)
- User organizations are responsible for notifying INAP of changes made to technical or administrative contact information. (criteria CC5.2, CC5.4, CC5.5)
- User organizations are responsible for ensuring their employees properly lock their cage or cabinet before leaving INAP facilities. (criteria CC5.5)
- User organizations are responsible for applying logical access security controls, data encryption controls, and related procedures to their network connected equipment. (criteria CC5.1, CC5.2, CC5.3, CC5.4, CC5.6, and CC5.7)
- User organizations are responsible for protecting their equipment against infection by computer viruses, malicious codes, and unauthorized software. (criteria CC5.8)
- User organizations are responsible for protecting and maintaining the security of system resources (e.g., secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services). (criteria CC5.6, CC5.7, CC6.1, CC6.2)

- User organizations are responsible for maintaining their own system components and configurations. (criteria CC7.1, CC7.2, CC7.3, CC7.4)
- User organizations are responsible for maintaining, monitoring, and evaluating the capacity and usage of their systems' bandwidth and processing requirements. (criteria A1.1)User organizations are responsible for the logical protection of their data, including performing backup procedures and periodically testing system and data recovery plans as necessary. (criteria A1.2, A1.3)

IV. INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITORS

Introduction

The accompanying description of the SJE011 Flagship Data Center Services of INAP is intended to provide user organizations and their auditors with sufficient information to obtain an understanding of those aspects of the controls of INAP that may be relevant to their control structure. This document, when combined with an understanding of the controls in place by the client, is intended to assist in the assessment of the total control structure surrounding transactions processed through a Flagship Data Center Services system.

Our review of the controls as described below for the period October 1, 2017 – September 30, 2018, included such tests as we considered necessary in the circumstances to obtain evidence about their effectiveness in meeting the control objectives specified. The procedures performed in our review include only testing or reviewing procedures with respect to the controls of the SJE011 Flagship Data Center Service operations of INAP. Consequently, we make no representations as to the adequacy of the control environment relative to other functions at INAP.

The objective of a control structure is to provide reasonable, but not absolute, assurance as to the safeguarding of assets against loss from unauthorized use or disposition and the reliability of records. The concept of reasonable assurance recognizes that the cost of a control structure should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgment made by management. As part of our study of the control structure, we performed a variety of tests, each of which provided different levels of audit satisfaction. The results of these tests provided the basis for our understanding of the control structure, and whether the controls included in this document were in place and operating effectively to ensure that transactions were being processed in accordance with INAP's controls. The section below outlines the various tests applied.

Our examination of the operating effectiveness of the controls of INAP's SJE011 Flagship Data Center services was restricted to selected control objectives as outlined below. The examination was performed in accordance with AICPA Statement on Standards for Attestation Engagements No. 18, *"Clarification and Recodification."* It is each user entity's responsibility to evaluate this information in relation to the control structure surrounding the specific client under audit.

Control Environment

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls.

Our tests of the control environment included the following procedures, to the extent we considered necessary: (a) a review of INAP's organizational structure, including the segregation of functional responsibilities, policy statements, accounting and processing manuals, personnel policies and the internal audit's policies; (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of our testing of their controls to support our conclusions on the achievement of selected control objectives.

Control Objectives, Control Activities, Testing Performed and Testing Results

Our testing of the effectiveness of controls included the testing necessary, based upon our judgment, to evaluate whether adherence with those controls was sufficient to provide reasonable, but not absolute, assurance that the specified control objectives included below were achieved during the period October 1, 2017 – September 30, 2018. In selecting particular tests of the effectiveness of controls, we considered (a) the nature of items being tested, (b) the types and competence of available evidential matter, (c) the nature of the control objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

The tests performed on the effectiveness of controls detailed in the following section are described below:

TEST	DESCRIPTION
Re-performance	Re-performed application of the control structure policy or procedure to ensure adequacy of its application. This includes, among other things, obtaining evidence of the arithmetical accuracy and correct processing of transactions by either re-computing INAP's computations or performing independent calculations.
Inspection	Inspected documents and reports that indicate performance of the control structure policy or procedures. This includes among other things: • Testing of source documents to ensure transactions processed were consistent with transaction requests and that such transactions were in compliance with control structure policies. • Reviewing of source documentation and authorization to verify propriety and timeliness of transactions processed.
Observation	Observed application of specific controls.
Inquiry	Made inquiries of the appropriate INAP staff. Inquiries seeking relevant information or representation from INAP personnel were performed to obtain: • Knowledge and additional information regarding the policy and procedure. • Corroborating evidence of the policy or procedure.

	INAP Control	Tests of Operating Effectiveness	Test Results
	Criteria Common to All Security and Availability Principles		
CC1.0	Common Criteria Related to Organization and Management		
CC1.1	**The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and availability.**		
	A - Organizational charts and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry and Inspection** Inquired to determine whether the organizational chart and job descriptions were updated within the past year. Inspected the organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.
CC1.2	**Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.**		
	A - Organizational charts and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry and Inspection** Inquired to determine whether the organizational chart and job descriptions were updated within the past year. Inspected the organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.
	B - The Data Center Operations Manual and Security Standard Operating Procedures (SOP) are reviewed and approved by Data Center Operations management on an annual basis.	**Inquiry and Inspection** Inquired about Data Center Operations Manual reviews and approvals. Inspected management's review and approval of the Data Center Operations Manual and Security SOP to verify they were reviewed and approved by Data Center Operations management within the past year.	No exceptions noted.
	C - The Network Operations Center procedures are reviewed and approved by Network Operations Center (NOC) management on an annual basis.	**Inquiry and Inspection** Inquired about Network Operations Center reviews and approvals. Inspected management's review and approval of the Network Operations Center procedures to verify that they were reviewed and approved by the Network Operations Center (NOC) management within the past year.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	D - The Customer Service Manual is reviewed and approved by Colocation business unit management on an annual basis.	**Inquiry and Inspection** Inquired about Customer Service Manual reviews and approvals. Inspected management's review and approval of the Customer Service Manual to verify that it was reviewed and approved by business unit management within the past year.	No exceptions noted.
CC1.3	**The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.**		
	E - An employment pre-screening process is in place. It includes background, credit, and DMV checks (based on job requirements).	**Inquiry and Inspection** Inquired about employment pre-screening process. Inspected pre-screen results in employee files for a sample of employees hired during the period to verify that an employment pre-screening process is in place and includes background, credit, and DMV checks where applicable and based on job requirements.	No exceptions noted.
	G - The Company allows operating units to budget training for each employee to continue their education either virtually or locally, including maintenance of certifications.	**Inquiry and Inspection** Inquired about training budgets for employees. Inspected INAP's operating budget for the current year to determine whether it included an allowance for training and continuing education.	No exceptions noted.
CC1.4	**The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.**		
	E - An employment pre-screening process is in place. It includes background, credit, and DMV checks (based on job requirements).	**Inquiry and Inspection** Inquired about employment pre-screening process. Inspected pre-screen results in employee files for a sample of employees hired during the period to verify that an employment pre-screening process is in place and includes background, credit, and DMV checks where applicable and based on job requirements.	No exceptions noted.
	H - The Company has a written Code of Conduct that is communicated to all employees. The Code details the company's expectations regarding behavior, ethics, and business practices that every employee must abide by.	**Inquiry, Observation, and Inspection** Inquired about the Code of Conduct. Observed the Code of Conduct on the Company intranet to verify that the Code of Conduct is communicated to all employees. Inspected the Code of Conduct to verify that it contains the company's expectations regarding behavior, ethics, and business practices.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC2.0	Common Criteria Related to Communications		
CC2.1	**Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.
	J - Customer on-boarding procedures include providing the new customer with a New Customer Guide, Customer Service Manual, and SLA upon initiating service.	**Inquiry and Inspection** Inquired of INAP personnel to determine whether new colocation customers are provided the New Customer Guide, Customer Service Manual, and Service Level Agreement upon initiating service. Inspected the New Customer Guide, Customer Service Manual, and Service Level Agreement to verify that they exist and include related availability and security obligations of users and INAP's availability and security commitments. Inspected an example e-mail for a new customer to verify that procedures exist to instruct the business unit to provide the New Customer Guide, Customer Service Manual, and Service Level Agreement to new customers.	No exceptions noted.
CC2.2	**The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	J - Customer on-boarding procedures include providing the new customer with a New Customer Guide, Customer Service Manual, and SLA upon initiating service.	**Inquiry and Inspection** Inquired of INAP personnel to determine whether new colocation customers are provided the New Customer Guide, Customer Service Manual, and Service Level Agreement upon initiating service. Inspected the New Customer Guide, Customer Service Manual, and Service Level Agreement to verify that they exist and include related availability and security obligations of users and INAP's availability and security commitments. Inspected an example e-mail for a new customer to verify that procedures exist to instruct the business unit to provide the New Customer Guide, Customer Service Manual, and Service Level Agreement to new customers.	No exceptions noted.
CC2.3	**The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.**		
	A - Organizational charts and job descriptions are in place and assign responsibility and accountability for system availability and security.	**Inquiry and Inspection** Inquired to determine whether the organizational chart and job descriptions were updated within the past year. Inspected the organizational chart and job descriptions to verify that the Company assigned responsibility and accountability for system availability and security.	No exceptions noted.
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	J - Customer on-boarding procedures include providing the new customer with a New Customer Guide, Customer Service Manual, and SLA upon initiating service.	**Inquiry and Inspection** Inquired of INAP personnel to determine whether new colocation customers are provided the New Customer Guide, Customer Service Manual, and Service Level Agreement upon initiating service. Inspected the New Customer Guide, Customer Service Manual, and Service Level Agreement to verify that they exist and include related availability and security obligations of users and INAP's availability and security commitments. Inspected an example e-mail for a new customer to verify that procedures exist to instruct the business unit to provide the New Customer Guide, Customer Service Manual, and Service Level Agreement to new customers.	No exceptions noted.
CC2.4	**Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.
	J - Customer on-boarding procedures include providing the new customer with a New Customer Guide, Customer Service Manual, and SLA upon initiating service.	**Inquiry and Inspection** Inquired of INAP personnel to determine whether new colocation customers are provided the New Customer Guide, Customer Service Manual, and Service Level Agreement upon initiating service. Inspected the New Customer Guide, Customer Service Manual, and Service Level Agreement to verify that they exist and include related availability and security obligations of users and INAP's availability and security commitments. Inspected an example e-mail for a new customer to verify that procedures exist to instruct the business unit to provide the New Customer Guide, Customer Service Manual, and Service Level Agreement to new customers.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC2.5	**Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.
	K - The process for users (customers) to inform the entity of system availability issues, possible security breaches, and other incidents is documented in the Customer Service Manual.	**Inquiry and Inspection** Inquired about the Customer Service Manual and the process for customers to report issues. Inspected the Colocation Customer Service Manual to verify that the process for customers to inform INAP of system availability issues, possible security breaches, and other incidents was documented.	No exceptions noted.
CC2.6	**System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.**		
	L - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	**Inquiry and Inspection** Inquired about the Critical Environment Work Authorization process and customer notification for scheduled maintenance and other relevant changes. Inspected Critical Environment Work Authorization (CEWA) and DATC forms for a sample of data center changes during the period to verify that the work had been properly documented and authorized. Inspected tickets documenting customer notifications for a sample of data center changes during the period to verify that customers were notified in advance of the maintenance or change.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls		
CC3.1	**The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.**		
	M - A third-party security risk assessment expert performs an enterprise wide risk assessment annually to identify potential security threats. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about third-party security risk assessments. Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
	N - Periodically, the Company performs a risk assessment to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about internal risk assessments. Inspected reports and results from the latest data center risk assessment and annual data center strategy plans to verify that a data center risk assessment had been performed and risks assessed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
CC3.2	**The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.

INAP Control	Tests of Operating Effectiveness	Test Results
M - A third-party security risk assessment expert performs an enterprise wide risk assessment annually to identify potential security threats. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about third-party security risk assessments. Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
N - Periodically, the Company performs a risk assessment to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about internal risk assessments. Inspected reports and results from the latest data center risk assessment and annual data center strategy plans to verify that a data center risk assessment had been performed and risks assessed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
O - Network Operations Center Procedures and a Customer Service Manual are in place documenting data center policies and procedures.	**Inquiry and Inspection** Inquired about Network Operations Center Procedures and the Customer Service Manual. Inspected the Network Operations Center Procedures listing and the Customer Service Manual to verify that data center security and availability policies and procedures are documented and in place.	No exceptions noted.
Q - The Company has an Internal Audit Department that monitors the design and operating effectiveness of controls related to security and availability commitments. Company management, with the assistance of Internal Audit, develops action plans related to observed deficiencies in the design and operating effectiveness of controls.	**Inquiry and Inspection** Inquired about the Internal Audit Department and action plans for control deficiencies. Inspected the Internal Audit Charter and Internal Audit workpapers to verify that the Company's Internal Audit Department monitors the design and effectiveness of operational controls, which would include those related to security and availability commitments. Inspected the action plans developed by Company management to verify that observed deficiencies in the design and operating effectiveness of controls are actively addressed by Company management.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC4.0	Common Criteria Related to Monitoring of Controls		
CC4.1	**The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.**		
	Q - The Company has an Internal Audit Department that monitors the design and operating effectiveness of controls related to security and availability commitments. Company management, with the assistance of Internal Audit, develops action plans related to observed deficiencies in the design and operating effectiveness of controls.	**Inquiry and Inspection** Inquired about the Internal Audit Department and action plans for control deficiencies. Inspected the Internal Audit Charter and Internal Audit workpapers to verify that the Company's Internal Audit Department monitors the design and effectiveness of operational controls, which would include those related to security and availability commitments. Inspected the action plans developed by Company management to verify that observed deficiencies in the design and operating effectiveness of controls are actively addressed by Company management.	No exceptions noted.
CC5.0	Common Criteria Related to Logical and Physical Access Controls		
CC5.1	**Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.**		
	R - Access to the keycard system and Ubersmith applications is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	**Inquiry and Inspection** Inquired about access to the keycard systems and Ubersmith application. Inspected the list of usernames and login screens for the keycard systems to verify that the applications were ID and password protected. Inspected the login screen for Ubersmith to verify that the applications were ID and password protected. Inspected the roles and privileges tables established for the keycard system and for Ubersmith to verify that privileges and authorizations associated with user accounts provided access based on the user's role.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	JJ - Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO Office and network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired about network monitoring tools and issue resolution. Inspected log reporting configurations for firewalls to verify that firewall logs are reported to the third party network monitoring vendor for review and monitoring. Inspected a sample of invoices for the third party network monitoring services vendor to verify that these services were performed throughout the period. Inspected e-mail alert configurations for the CISO Office and network engineering group to verify that these personnel are notified of critical events in real time. Inspected the list of open security issues and incidents to verify that events that may affect data center security were documented, tracked, and monitored until incident resolution.	No exceptions noted.
CC5.2	**New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.**		
	U - Data Center Management approves all provisioning of Administrator access (add, modify, delete users) to the keycard system.	**Inquiry and Inspection** Inquired about the provisioning of administrator access to the keycard system. Inspected a sample of approvals for administrative users added during the period to verify that access was approved by Data Center Management.	No exception noted.
	V - On a quarterly basis, individuals with access to add, modify, and delete users in the keycard system are reviewed for appropriateness.	**Inquiry and Inspection** Inquired about administrator access reviews. Inspected a sample of quarterly audits to verify that INAP colocation security personnel perform quarterly audits to validate the appropriateness of individuals with access to add, modify, and delete users in the key card access system.	No exception noted.

INAP Control	Tests of Operating Effectiveness	Test Results
W - User access to edit the Facilities Access Customer Contact Lists in Ubersmith is reviewed for appropriateness based on job responsibilities on an annual basis.	**Inquiry and Inspection** Inquired about reviews of user access to edit the Facilities Access Customer Contact Lists in Ubersmith. Inspected the annual review of user access to edit the customer contact lists to verify that INAP personnel performed an annual review to validate the appropriateness of individuals with access to edit the customer contact lists in Ubersmith. Inspected the list of active users with access to edit the customer contact lists to verify that any users with inappropriate access to the system identified during the annual review were removed.	No exceptions noted.
X - User access to INAP internal systems that support the keycard system and Ubersmith Facilities Access Customer Contact Listing is removed for terminated employees in a timely manner.	**Inquiry and Inspection** Inquired of IT management to verify that procedures are in place related to the removal of terminated employees from INAP systems, including the keycard system and Ubersmith applications. Inspected the user access listings to the INAP internal network for a sample of terminated employees with access to the keycard system, Ubersmith Facilities Access Customer Contact Listing, and supporting IT infrastructure to verify that access was revoked for these terminated employees. Inspected the help desk tickets documenting access removal for a sample of terminated employees with access to the keycard system, Ubersmith Facilities Access Customer Contact Listing, and supporting IT infrastructure to verify that terminated employees were removed from these systems in a timely manner.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC5.3	**Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.**		
	R - Access to the keycard system and Ubersmith applications is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	**Inquiry and Inspection** Inquired about access to the keycard systems and Ubersmith application. Inspected the list of usernames and login screens for the keycard systems to verify that the applications were ID and password protected. Inspected the login screen for Ubersmith to verify that the applications were ID and password protected. Inspected the roles and privileges tables established for the keycard system and for Ubersmith to verify that privileges and authorizations associated with user accounts provided access based on the user's role.	No exceptions noted.
	S - Password length and complexity requirements are established for the INAP internal network. Network passwords must be changed every 90 days. Account lockout features are set to lock out or disable a user after a number of failed login attempts to the network.	**Inquiry and Inspection** Inquired about network password standards and lockout features. Inspected the password settings established for the network to verify that minimum length, complexity, and change requirements are in place for network account passwords. Inspected the account lockout settings established for Active Directory to verify that users are locked out or disabled after a number of failed login attempts.	No exceptions noted.
	T - Password settings for the Ubersmith application include length and change requirements. Account lockout features are set to lock out or disable a user after a number of failed login attempts to the Ubersmith application. Password settings and account lockout features for the keycard system are the same as for Active Directory since the system uses single sign on.	**Inquiry, Observation, and Inspection** Inquired about application password standards and lockout features. Observed a user sign in to the keycard system to verify that the keycard system uses single sign on with Active Directory and that their password would be subject to the same requirements as those established by the network. Inspected the password settings established for the Ubersmith application to verify that minimum length and change requirements are in place for Ubersmith application passwords. Inspected evidence of the account lockout settings established for the Ubersmith application to verify that users are locked out or disabled after a number of failed login attempts.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	Y - In order to gain physical access to INAP data centers, employees and customers must be validated via a combination of key card and/or biometric technology.	**Inquiry and Observation** Inquired of management to determine whether employees and customers must be validated by key card and biometric technology. Observed successful and unsuccessful attempts to gain entry to the data center to verify that employees and customers must be validated by keycard and/or biometric technology.	No exceptions noted.
CC5.4	**Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.**		
	R - Access to the keycard system and Ubersmith applications is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	**Inquiry and Inspection** Inquired about access to the keycard systems and Ubersmith application. Inspected the list of usernames and login screens for the keycard systems to verify that the applications were ID and password protected. Inspected the login screen for Ubersmith to verify that the applications were ID and password protected. Inspected the roles and privileges tables established for the keycard system and for Ubersmith to verify that privileges and authorizations associated with user accounts provided access based on the user's role.	No exceptions noted.
	U - Data Center Management approves all provisioning of Administrator access (add, modify, delete users) to the keycard system.	**Inquiry and Inspection** Inquired about the provisioning of administrator access to the keycard system. Inspected a sample of approvals for administrative users added during the period to verify that access was approved by Data Center Management.	No exception noted.
	V - On a quarterly basis, individuals with access to add, modify, and delete users in the keycard system are reviewed for appropriateness.	**Inquiry and Inspection** Inquired about administrator access reviews. Inspected a sample of quarterly audits to verify that INAP colocation security personnel perform quarterly audits to validate the appropriateness of individuals with access to add, modify, and delete users in the key card access system.	No exception noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	W - User access to edit the Facilities Access Customer Contact Lists in Ubersmith is reviewed for appropriateness based on job responsibilities on an annual basis.	**Inquiry and Inspection** Inquired about reviews of user access to edit the Facilities Access Customer Contact Lists in Ubersmith. Inspected the annual review of user access to edit the customer contact lists to verify that INAP personnel performed an annual review to validate the appropriateness of individuals with access to edit the customer contact lists in Ubersmith. Inspected the list of active users with access to edit the customer contact lists to verify that any users with inappropriate access to the system identified during the annual review were removed.	No exceptions noted.
CC5.5	**Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.**		
	Y - In order to gain physical access to INAP data centers, employees and customers must be validated via a combination of key card and/or biometric technology.	**Inquiry and Observation** Inquired of management to determine whether employees and customers must be validated by key card and biometric technology. Observed successful and unsuccessful attempts to gain entry to the data center to verify that employees and customers must be validated by keycard and/or biometric technology.	No exceptions noted.
	Z - Customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Lock mechanisms are combination, badge reader, or physical key.	**Inquiry and Observation** Inquired of data center management to determine whether customer equipment is segregated via locked cages or locked cabinets to ensure that customers can only access their own equipment. Observed locked cages and locked cabinets to verify that customer equipment was segregated via locked cages or locked cabinets such that customers could only access their own equipment.	No exceptions noted.
	AA - INAP data centers are monitored and manned 24/7/365. Entry is validated by keycard and / or biometric technology and documented by the ACS, visitor and camera logs.	**Inquiry and Observation** Inquired of data center management to determine whether a manned security post controls entry into INAP data centers. Observed the manned security post that is placed in line of sight of where customers gain access to the data center to verify that a manned security post controlled entry into the data center.	No exceptions noted.

INAP Control	Tests of Operating Effectiveness	Test Results
BB - Visitor access to INAP data centers is logged at the security desk.	**Inquiry, Observation, and Inspection** Inquired about the logging of visitor access to INAP data centers. Observed data center visitor logs to verify that access to INAP data centers was logged. Inspected the visitor logs to verify that details of visitor access to INAP Data Centers is logged at the security desk.	No exceptions noted.
DD - Only authorized INAP employees, contractors, security guards, and customers are granted physical access to the data center.	**Inquiry and Inspection** Inquired about physical access authorization for data centers. Inspected a sample of approvals for employees, contractors, security guards, and customers who were granted physical access to the data center during the period to verify that only authorized INAP employees, contractors, security guards, and customers are granted physical access to the data center.	No exceptions noted.
FF - INAP colocation security personnel perform a quarterly audit to validate the appropriateness of all customers' physical access to the data centers.	**Inquiry and Inspection** Inquired about verification of physical access to data centers for customers. Inspected a sample of quarterly customer access audits to verify that INAP colocation security personnel perform a quarterly audit to validate the appropriateness of customers' physical access to the data centers.	No exceptions noted.
GG - Physical access to the data center is revoked upon termination of INAP employees, contractors, and security guards.	**Inquiry and Inspection** Inquired about physical access revocation for terminated employees. Inspected the active keycard listing for a sample of terminated employees and security guards to verify that physical access to the data center is revoked upon termination of INAP employees, contractors, and security guards.	No exceptions noted.
HH - Physical access to the data center is revoked upon notification by customers to the NOC for customer employee terminations.	**Inquiry and Inspection** Inquired about physical access revocation for terminated customer employees. Inspected the keycard access listings for a sample of customer employees who required data center access revocation to verify that unauthorized customer employee access was removed.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC5.6	**Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.**		
	II - The Company has firewalls in place to limit access over the internet to the central keycard system application and database.	**Inquiry and Inspection** Inquired about company firewalls. Inspected firewall logging rules to verify the presence of firewalls protecting the keycard system application and database.	No exceptions noted.
	JJ - Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO Office and network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired about network monitoring tools and issue resolution. Inspected log reporting configurations for firewalls to verify that firewall logs are reported to the third party network monitoring vendor for review and monitoring. Inspected a sample of invoices for the third party network monitoring services vendor to verify that these services were performed throughout the period. Inspected e-mail alert configurations for the CISO Office and network engineering group to verify that these personnel are notified of critical events in real time. Inspected the list of open security issues and incidents to verify that events that may affect data center security were documented, tracked, and monitored until incident resolution.	No exceptions noted.
CC5.7	**The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.**		
	R - Access to the keycard system and Ubersmith applications is ID and password protected. Roles based access ensures privileges and authorizations associated with user accounts provide access to specific limited system functionality.	**Inquiry and Inspection** Inquired about access to the keycard systems and Ubersmith application. Inspected the list of usernames and login screens for the keycard systems to verify that the applications were ID and password protected. Inspected the login screen for Ubersmith to verify that the applications were ID and password protected. Inspected the roles and privileges tables established for the keycard system and for Ubersmith to verify that privileges and authorizations associated with user accounts provided access based on the user's role.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	KK - Connections via VPN tunnel between the central physical access systems and each data center are protected using encryption.	**Inquiry, Observation, and Inspection** Inquired about encryption for VPN connections. Observed encryption configurations during an onsite demonstration Inspected the VPN tunnel encryption configurations to verify that VPN connections between the central keycard system and each data center are appropriately configured with encryption technology.	No exceptions noted.
	AAA - Connections to the Ubersmith application via the internet are protected using encryption.	**Inquiry and Inspection** Inquired about encryption for connections to the Ubersmith application. Inspected a screenshot of the Ubersmith login screen and determined that encryption was being used, as evidenced that the site URL included HTTPS instead of HTTP.	No exceptions noted.
CC5.8	**Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.**		
	LL - Anti-virus software for network workstations and keycard system servers is installed and operating effectively.	**Inquiry and Inspection** Inquired about anti-virus software for network workstations and keycard system servers. Inspected the anti-virus policy settings to verify that the version and virus dictionary for network workstations and keycard system servers were properly maintained.	No exceptions noted.
	JJ - Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO Office and network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired about network monitoring tools and issue resolution. Inspected log reporting configurations for firewalls to verify that firewall logs are reported to the third party network monitoring vendor for review and monitoring. Inspected a sample of invoices for the third party network monitoring services vendor to verify that these services were performed throughout the period. Inspected e-mail alert configurations for the CISO Office and network engineering group to verify that these personnel are notified of critical events in real time. Inspected the list of open security issues and incidents to verify that events that may affect data center security were documented, tracked, and monitored until incident resolution.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC6.0	Common Criteria Related to System Operations		
CC6.1	**Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.**		
	M - A third-party security risk assessment expert performs an enterprise wide risk assessment annually to identify potential security threats. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about third-party security risk assessments. Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
	N - Periodically, the Company performs a risk assessment to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about internal risk assessments. Inspected reports and results from the latest data center risk assessment and annual data center strategy plans to verify that a data center risk assessment had been performed and risks assessed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
	JJ - Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO Office and network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired about network monitoring tools and issue resolution. Inspected log reporting configurations for firewalls to verify that firewall logs are reported to the third party network monitoring vendor for review and monitoring. Inspected a sample of invoices for the third party network monitoring services vendor to verify that these services were performed throughout the period. Inspected e-mail alert configurations for the CISO Office and network engineering group to verify that these personnel are notified of critical events in real time. Inspected the list of open security issues and incidents to verify that events that may affect data center security were documented, tracked, and monitored until incident resolution.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	MM - The Network Operations Center (NOC) tracks data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired of the DC Facilities team to verify that procedures are in place related to tracking, escalating, and managing incidents that may affect data center availability. Inspected a sample of NOC tickets documenting availability related incidents to verify that incidents that may affect data center availability were documented, tracked, and monitored until incident resolution.	No exceptions noted.
	NN - For serious incidents that may affect data center availability, an Event Report is prepared by Data Center Operations personnel. These reports include a root cause analysis and corrective action plans, when applicable. Corrective action plans are implemented as deemed necessary by management.	**Inquiry and Inspection** Inquired of Data Center Operations management regarding the nature of any serious incidents that occurred during the period. Inspected Event Reports for any serious incidents that occurred during the period to verify that the incidents were documented and included a root cause analysis and corrective action plans, when applicable.	No exceptions noted.
CC6.2	**Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.**		
	I - Each INAP Company controlled data center has a detailed Operations Manual which is available and communicated to all users (emergency procedures are documented within).	**Inquiry, Observation, and Inspection** Inquired about the Data Center Operations Manual. Observed the Data Center Operation Manual on the Company intranet to verify that the manual is available and communicated to INAP employees and other internal users. Inspected the Data Center Operations Manual to verify that it contained relevant content, including emergency procedures for the data center.	No exceptions noted.
	CC - INAP employs 24 hour video surveillance to monitor all entrances, exits, and other sensitive areas of its data centers. Surveillance video footage is retained for at least 90 days.	**Inquiry and Observation** Inquired about video surveillance of data centers. Observed video surveillance cameras at entrances, exits, and sensitive areas, as well as security personnel monitoring video feeds, to verify that entrances, exits, and sensitive areas of the data center were monitored. Observed historical surveillance video footage to verify that recordings were retained for at least 90 days.	No exceptions noted.

INAP Control	Tests of Operating Effectiveness	Test Results
JJ - Network monitoring tools are in place to detect unauthorized access to the network. Critical alerts are sent real time to the CISO Office and network engineering group for follow-up and resolution. Issues and incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired about network monitoring tools and issue resolution. Inspected log reporting configurations for firewalls to verify that firewall logs are reported to the third party network monitoring vendor for review and monitoring. Inspected a sample of invoices for the third party network monitoring services vendor to verify that these services were performed throughout the period. Inspected e-mail alert configurations for the CISO Office and network engineering group to verify that these personnel are notified of critical events in real time. Inspected the list of open security issues and incidents to verify that events that may affect data center security were documented, tracked, and monitored until incident resolution.	No exceptions noted.
MM - The Network Operations Center (NOC) tracks data center power, environmental, and other incidents that may affect data center availability. Incidents are escalated as necessary and tracked until resolution.	**Inquiry and Inspection** Inquired of the DC Facilities team to verify that procedures are in place related to tracking, escalating, and managing incidents that may affect data center availability. Inspected a sample of NOC tickets documenting availability related incidents to verify that incidents that may affect data center availability were documented, tracked, and monitored until incident resolution.	No exceptions noted.
PP - A smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire.	**Inquiry and Observation** Inquired about data center smoke detection devices. Observed the smoke detection system in the data center to verify that a smoke detection system was installed in the data center.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
CC7.0	Common Criteria Related to Change Management		
CC7.1	**The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.**		
	L - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	**Inquiry and Inspection** Inquired about the Critical Environment Work Authorization process and customer notification for scheduled maintenance and other relevant changes. Inspected Critical Environment Work Authorization (CEWA) and DATC forms for a sample of data center changes during the period to verify that the work had been properly documented and authorized. Inspected tickets documenting customer notifications for a sample of data center changes during the period to verify that customers were notified in advance of the maintenance or change.	No exceptions noted.
CC7.2	**Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.**		
	M - A third-party security risk assessment expert performs an enterprise wide risk assessment annually to identify potential security threats. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about third-party security risk assessments. Inspected reports and results from the latest enterprise wide risk assessment to verify that an enterprise wide risk assessment was completed and reviewed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.
	N - Periodically, the Company performs a risk assessment to identify potential threats of disruption. The results of the latest risk assessment are revisited annually to assess the risk associated with the threats identified. Improvements to controls are prioritized and budgeted for by Company management.	**Inquiry and Inspection** Inquired about internal risk assessments. Inspected reports and results from the latest data center risk assessment and annual data center strategy plans to verify that a data center risk assessment had been performed and risks assessed within the past year. Inspected budgeting and planning worksheets to verify that improvements to controls are prioritized and budgeted for by Company management.	No exceptions noted.

	INAP Control	Tests of Operating Effectiveness	Test Results
	NN - For serious incidents that may affect data center availability, an Event Report is prepared by Data Center Operations personnel. These reports include a root cause analysis and corrective action plans, when applicable. Corrective action plans are implemented as deemed necessary by management.	**Inquiry and Inspection** Inquired of Data Center Operations management regarding the nature of any serious incidents that occurred during the period. Inspected Event Reports for any serious incidents that occurred during the period to verify that the incidents were documented and included a root cause analysis and corrective action plans, when applicable.	No exceptions noted.
CC7.3	**Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.**		
	NN - For serious incidents that may affect data center availability, an Event Report is prepared by Data Center Operations personnel. These reports include a root cause analysis and corrective action plans, when applicable. Corrective action plans are implemented as deemed necessary by management.	**Inquiry and Inspection** Inquired of Data Center Operations management regarding the nature of any serious incidents that occurred during the period. Inspected Event Reports for any serious incidents that occurred during the period to verify that the incidents were documented and included a root cause analysis and corrective action plans, when applicable.	No exceptions noted.
	Q - The Company has an Internal Audit Department that monitors the design and operating effectiveness of controls related to security and availability commitments. Company management, with the assistance of Internal Audit, develops action plans related to observed deficiencies in the design and operating effectiveness of controls.	**Inquiry and Inspection** Inquired about the Internal Audit Department and action plans for control deficiencies. Inspected the Internal Audit Charter and Internal Audit workpapers to verify that the Company's Internal Audit Department monitors the design and effectiveness of operational controls, which would include those related to security and availability commitments. Inspected the action plans developed by Company management to verify that observed deficiencies in the design and operating effectiveness of controls are actively addressed by Company management.	No exceptions noted.
		Inquired about testing and confirmation of backup power systems' operating effectiveness. Inspected load bank testing and/or other testing documentation to verify that backup power system effectiveness was confirmed within the past year.	

	INAP Control	Tests of Operating Effectiveness	Test Results
CC7.4	**Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.**		
	L - The Company has in place a Critical Environment Work Authorization (CEWA) process to ensure all scheduled maintenance and other data center implementations / modifications are properly documented and authorized to assure minimal impact to customers. For scheduled maintenance and other changes that have the potential to affect customer availability, customers are notified of the maintenance or change in advance.	**Inquiry and Inspection** Inquired about the Critical Environment Work Authorization process and customer notification for scheduled maintenance and other relevant changes. Inspected Critical Environment Work Authorization (CEWA) and DATC forms for a sample of data center changes during the period to verify that the work had been properly documented and authorized. Inspected tickets documenting customer notifications for a sample of data center changes during the period to verify that customers were notified in advance of the maintenance or change.	No exceptions noted.
A1.1	**Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.**		
	OO - Data center power and cooling capacity reports are prepared on a monthly basis to assist Data Center Operations management in maintaining, monitoring, and evaluating power and cooling capacity needs.	**Inquiry and Inspection** Inquired about data center power and cooling capacity reports. Inspected a sample of data center power and cooling capacity reports to verify that power and cooling capacity needs were maintained, monitored, and evaluated on a monthly basis, at a minimum.	No exceptions noted.
A1.2	**Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.**		
	PP - A smoke detection system is installed in the data center to detect and alert data center personnel to the presence of a fire.	**Inquiry and Observation** Inquired about data center smoke detection devices. Observed the smoke detection system in the data center to verify that a smoke detection system was installed in the data center.	No exceptions noted.
	QQ - The smoke detection system is inspected and serviced at least annually to ensure effective operation.	**Inquiry and Inspection** Inquired about inspection and servicing of smoke detection system. Inspected preventative maintenance and inspection reports to verify that smoke detection systems were inspected and serviced within the past year.	No exceptions noted.

INAP Control	Tests of Operating Effectiveness	Test Results
RR - The data center is protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers located throughout the data center.	**Inquiry and Observation** Inquired about data center fire protection devices. Observed fire suppression systems and fire extinguishers throughout the data center to verify that the data center was protected from the risk of fire by a pre-action, dry pipe sprinkler fire suppression system, as well as fire extinguishers.	No exceptions noted.
SS - The pre-action, dry pipe sprinkler fire suppression system is inspected and serviced at least annually, and fire extinguishers are inspected and serviced at least annually, to ensure effective operation.	**Inquiry and Inspection** Inquired about inspection and servicing of fire protection devices. Inspected preventive maintenance and inspection reports to verify that the fire suppression system and fire extinguishers were inspected and serviced within the past year.	No exceptions noted.
TT - Multiple HVAC units control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	**Inquiry and Observation** Inquired about data center HVAC units. Observed multiple HVAC units to verify that HVAC units were designed to control both temperature and humidity within the data center, delivering redundant HVAC service throughout the data center.	No exceptions noted.
UU - HVAC units are inspected and serviced at least annually to ensure effective operation.	**Inquiry and Inspection** Inquired about inspection and servicing of HVAC units. Inspected preventative maintenance and inspection reports to verify that HVAC units were inspected and serviced within the past year.	No exceptions noted.
VV - Redundant UPS systems are in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	**Inquiry and Observation** Inquired about redundant UPS systems in data centers. Observed UPS systems to verify that redundant UPS systems were in place to provide temporary power in the event of a power failure and to mitigate the risk of power surges impacting infrastructure in the data center.	No exceptions noted.
WW - UPS systems are inspected and serviced at least annually to ensure effective operation.	**Inquiry and Inspection** Inquired about inspection and servicing of UPS systems. Inspected preventative maintenance and inspection reports to verify that UPS systems were inspected and serviced within the past year.	No exceptions noted.