Houston County Commissioners

Purchasing Department

Director of Purchasing

Vanessa Zimmerman

Office

200 Carl Vinson Parkway
Warner Robins, GA 31088

478-236-1700

April 14, 2025

Dear Vendor:

The Houston County Board of Commissioners is soliciting sealed proposals for an **Emergency Notification System** for use by the Houston County Emergency Management Agency and Houston County Emergency Communications. Our minimum specifications and instructions are attached.

To receive consideration, your sealed proposal will be accepted at the Purchasing Department office **ONLY**, located at 200 Carl Vinson Parkway, Warner Robins, Georgia 31088, until 5:00 p.m. on Tuesday, April 29, 2025.

Your sealed proposal package **MUST** be marked:

SEALED PROPOSAL #25-13 Emergency Notification System

and received at the above address before the 5:00 p.m. deadline on Tuesday, April 29, 2025.

Proposals will be evaluated, recapped, and presented to the Board of Commissioners during their regularly scheduled meeting on Tuesday, May 20, 2025, at 5:00 p.m. at the Houston County Annex in Warner Robins, Georgia. Award will be based on the best value to Houston County.

HOUSTON COUNTY RESERVES THE RIGHT TO ACCEPT NONE, ALL OR ANY PART OF YOUR PROPOSAL AND WAIVE ALL INFORMALITIES.

Sincerely,

VANESSA ZIMMERMAN
DIRECTOR OF PURCHASING
HOUSTON COUNTY BOARD OF COMMISSIONERS

Enclosures

[HOUSTON COUNTY, GA]

"Emergency Notification System (ENS)"

Request for Proposal

Date Posted: APRIL 15, 2025

Contents

Purpose 2
Evaluation and Award Criteria 2
Background 3
Proposal Preparation and Submission Guidelines 3
Contact Info 3
Statement of Needs 4
1. General Requirements Overview 4
2. Vendor Information 4
3. Messaging Infrastructure and Scalability 5
4. Citizen / Resident Registration and Notification 7
5. Location- and Map-Based Alerting Interfaces 10
6. Mobile Applications and Location-Based Messaging 14
7. Emergency Management Decision Support 18
8. General Messaging 20
9. Internal Employee, Staff and Operational User Messaging 26
10. User Management 28
11. Safety Responder Collaboration, Coordination and Event Communications 30
12. Integrations and Partner Ecosystem 32
13. Implementation, Training and Support 34
14. Product Roadmap, Other Capabilities and Future Enhancements 35
15. Information Security and Data Privacy 36
Pricing 41

Purpose

The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified sources to establish a contract through competitive negotiations to provide an Emergency Notification System (ENS) for [Houston County, GA]. This system will be used to allow any member of the public to provide critical information about themselves, their families and households for use during emergency management planning, response and recovery activities. Emergency management officials will be provided with real-time, web-based access to this information, and a fully integrated emergency notification system to rapidly notify the public, enabling them to respond quickly and safely to any emergency incidents affecting the jurisdiction. The emergency notification system must at minimum support notification via SMS, email, voice, mobile applications, IPAWS and social media. The ENS will be a key component of our jurisdiction's emergency preparedness and communication strategy.

Evaluation and Award Criteria

Responses to this RFP will be evaluated based on the vendor's ability to:

- Meet the minimum required functionality
- Demonstrate robustness/redundancy of infrastructure, allowing for high availability of data and high rates of message delivery
- Provide additional capabilities deemed to be valuable to meeting the overall objectives of enhancing whole community preparedness
- Provide support and training services needed to ensure program success
- Provide client references specific to the product and services required
- Demonstrate focus on emergency management, public safety, and messaging requirements
- Overall price

Houston County reserves the right to accept or reject all proposals based on the above abilities.

Background

Houston County is one of the fastest growing counties in Georgia with an estimated population of 175,000. Houston County is home to Robins AFB and the cities of Warner Robins, Perry, and Centerville. To ensure fiscal responsible practices we are issuing this Request for Proposals. Mass notifications are managed primarily through the Houston County Emergency Management Agency and Houston County Emergency Communications. Proposal review committee will be comprised of members from each of these agencies.

Proposal Preparation and Submission Guidelines

Proposals should be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

Information which the vendor desires to present that does not fall within any of the requirements of the RFP should be inserted at the appropriate place or be attached at the end of the proposal and designated as additional material and/or optional features or services. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

As used in this RFP, the terms **"must", "shall", "should"** and **"may**" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the vendor solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have a large impact and would be useful but are not necessary. Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of a vendor to satisfy a "must" or "shall" requirement does not automatically remove that vendor from consideration; however, it may seriously affect the overall rating of the vendor's proposal.

Timeline for this procurement and implementation process is as follows:

1) Initial request for proposals 4-15-2025
2) Submissions by 4-29-2025 at 5:00 PM time
3) Finalists announced 4-30-2025
4) Follow up meetings and demonstrations (Virtual) 5-1-2025 & 5-2-2025 (time slots will be emailed on 4-30-2025)
5) Vendor selection and contract execution complete 5-20-2025 at 5:00 PM Board of Commissioners Meeting
6) Expected implementation complete date: 7-1-2025 (Set up and Training in June 2025)

Contact Info

Provide contact information and availability information for jurisdiction's RFP lead procurement agent and/or primary points of contact

Software use questions:
Christopher Stoner, Chief
cstoner@houstoncountyga.gov
478-542-2026

General procurement questions:
Vanessa Zimmerman, Purchasing Director
vzimmerman@houstoncountyga.gov
478-236-1700

Statement of Needs

1. General Requirements Overview

Requirement	Response
1. Provide a high-level overview of the vendor solution and how it applies to the overall goals and requirements presented in this bid request.	

2. Vendor Information

Requirement	Response
1. Provide the primary point of contact and contact information for the Vendor, including name, title, email address	
2. Describe the Vendor's form of business (*i.e.*, individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and detail the name, mailing address, and telephone number of the person the Institution should contact regarding the proposal.	
3. Provide a Statement of whether the Vendor or any of the Vendor's employees, agents, independent contractors, or subcontractors have been convicted of, pled guilty to, or pled *nolo contendere* to any felony, and if so, an explanation providing relevant details.	
4. Provide a brief, descriptive Statement indicating the Vendor's credentials to deliver the services sought under this RFP.	
5. Indicate the Vendor organization's number of employees, client base, and location of offices.	
6. Provide an organization chart detailing how Vendor's organization is organized.	
7. Vendor must have provided similar services for a minimum of 10 years. Describe Vendor's experience delivering relevant solutions in jurisdictions of comparable size.	

8. Vendor must be able to warrant that they provide background checks on all employees, and that only employees who have undergone background checks will have access to data.	
9. What % of the proposing vendor's revenue is derived from sales to public safety organizations (versus private or other non-public-safety focused government solutions)?	
10. Provide a narrative description of the proposed project team and its organizational structure, listing its staff participants and short resumes noting the qualifications of key staff who will support the solution.	

3. Messaging Infrastructure and Scalability

Requirement	Response
1. Vendor solution must be cloud-hosted. Describe any on-site hardware or software installation required, or other deviations from a cloud-based / vendor-hosted / SaaS model.	
2. Provide an overview of the infrastructure platform used to deliver the vendor's solutions.	
3. Is any [Houston County, GA] data used for notifications dependent of third-party or contracted cloud infrastructure platforms (e.g., AWS, Azure, etc.)?If so, describe any redundancies in place to cover the event of a services outage.	
4. Are there any single points of failure in the messaging delivery between your hosting center and the "last mile" infrastructure (e.g., calling centers, SMS aggregator binds, email servers, etc.)? Describe how delivery risk is minimized along the message delivery chain for the different message types.	
5. How can [Houston County, GA] users be sure their information is privacy protected, will not be used for any other purpose or sold to third parties?The vendor solution must be free of advertisements.	

6. Describe how features and enhancements are identified, prioritized, and introduced.	
7. Vendor should describe their ongoing maintenance and system testing procedures. Include in this response information relative to how new features are addressed.	

8. Vendor solution must minimally support the following notification methods:
 	
• SMS via SMPP
• Email
• Outbound Dialed Voice
• Social Media (Twitter, Facebook)
• RSS feed
• Common Alerting Protocol (CAP)
  ○ CAP Producer role (activating other safety systems from Vendor's solution)
  ○ CAP Consumer role (activating Vendor solution from another safety system)
• Push Notifications to Mobile App(s)
• IPAWS
• Desktop notifications
• List any other supported modes	

9. Vendor solution must work across all major wireless carriers and wireless phone models. Describe any limitations and how the system addresses delivery to smaller carriers.	
10. Vendor must demonstrate an effective SMS delivery architecture. Describe your SMS delivery architecture. Do you deliver messages via SMTP or SMPP? If delivery is via SMTP only, please detail carrier whitelisting relationships. If SMPP, does your system utilized direct binds or aggregators? What safeguards are in place to ensure message delivery?	

4. Citizen / Resident Registration and Notification

Requirement	Response
1. Vendor's solution must include a hosted, web-based registration portal for citizens. Please provide a description of the citizen-facing opt-in / registration portal.	
2. Vendor's citizen registration portal must be compliant with Section 508 of the Americans with Disabilities Act and WCAG 2.0 or higher standards for product accessibility. Describe how the registration portal meets all applicable requirements. If available, please append a Voluntary Product Accessibility Template (VPAT) document for your solution.	
3. Vendor's citizen registration portal must provide both residents and commuters with the ability to create and maintain their account 24/7/365 via desktops, laptops, tablets, and/or mobile applications. Describe the citizen's ability to access the Vendor's registration portal.	
4. Vendor's registration portal must be fully compatible with registrations generated within a publicly available mobile application.	
5. Vendor's system must support customization of portal branding. Describe configuration options.	
6. Vendor's system must provide mechanisms to register for public alerts *without* requiring an email address.	
7. Vendor solution must support a mechanism to enable end-user *assistants / caregivers* to subscribe on behalf of members of the public who are unable to manage their own notification subscriptions online.	
8. Vendor's registration portal must be available in multiple languages. List supported languages.	
9. Vendor's solution must validate citizen entered telephone numbers through an automated telephone confirmation process. Describe validations performed on citizen-supplied contacts.	

10. Vendor's solution must validate address and location information to be consistent and accurate data.	
11. Vendor's solution must incorporate an automated system to keep data current in the system.	
12. Automated reminders sent to the citizen to update their information. These reminders must be delivered by the Vendor via no less than two modes of communication, such as text, email, voice call and/or push notifications to mobile devices.	
13. Vendor solution must implement an automated data-aging process to ensure the integrity of the data. Describe the Vendor's process(es) for identifying and addressing aging data.	
14. Vendor solution must allow subscribers to register, in a seamless manner, for offered by multiple Jurisdictions (i.e., State, county and local, 911,l, etc). For example, if citizens live in one jurisdiction and work in another that both offer opt-in services, they must be able to create a single account that is registered for both jurisdiction's offerings via a single login, and through a single page to manage opt-in preferences.	
15. Vendor's solution must offer the Jurisdiction the capability of customizing the question set and data fields that the citizen is presented with through the registration portal. Describe how the Vendor's solution provides for customization of data collection.	
16. Vendor solution must support unlimited addresses for subscribers, including residential as well as business addresses and commuter populations. Address information must be available for geographic as well as logical selections where appropriate.	
17. Vendor's solution must offer the ability for members of the public to opt-in to receive alerts by sending an SMS text message. Describe functionality and how it may be used: • As a generalized opt-in method • In support of community events • To enroll users on a temporary basis.	

18. Vendor's solution must be able customize message sent to subscriber when registering via SMS text message.	
19. Vendor's solution must automatically expire registrations made via SMS.	
20. Vendor's solution must allow citizens who register via SMS text message to unsubscribe via SMS message.	
21. Vendor's solution must allow the Jurisdiction to associate customized data collection with a given citizen registration entity, including: person, address, contact information, and more. Describe available data collection and any specific limitations on the number and/or types of contacts.	
22. Vendor solution must allow [Houston County, GA] to include organization-specific content and branding. Describe available functionality.	
23. Vendor solution must allow citizens to opt-in to emergency notification messages **by category**. How are categories created, managed, and presented to the end user subscriber?	
24. Vendor solution must allow [Houston County, GA] to define "non-emergency" topics for opt-in during registration.	
25. Citizens who opt-in to notification sub-categories must be automatically included to receive emergency notifications from [JURISDICTION].	
26. Vendor solution must allow registrants to identify the relationship between individuals, addresses, and contact information for the purpose of improving emergency management queries and targeting of notifications.	
27. Describe any services, features, or best practices to assist with marketing of the system to public subscribers.	

28. Vendor solution must support automated weather notifications. Describe features as well as any additional modules or costs required.	
29. Vendor solution must support geographic boundaries for predicted path weather notifications. Describe features as well as any additional modules or costs required.	
30. Vendor solution must provide a mechanism for citizens to opt-in or opt-out of weather notifications sent by the system.	

5. Location- and Map-Based Alerting Interfaces

Requirement	Response
1. Vendor must allow for the selection of users via a map-based interface. Describe controls and use models for location-targeted alerting.	
Functionality for Alert Administrators and Senders:	
2. Vendor solution must have the ability to search for a residence or business by searching for an address, landmark, or other commonly-used geographic search criteria.	
3. Vendor solution must support all features required for IPAWS geographic selection requirements.	
4. Must support jurisdiction access to IPAWS Labs Cloud test environment.	
5. Vendor must be listed on FEMA's List of Alert Origination Software Providers (AOSP), showing that the vendor has successfully demonstrated IPAWS functionality.	
6. Describe the strategies implemented by the Vendor solution to reduce the complexity IPAWS integration requirements and to prevent accidental activations and mistakes caused by human error?	

7. Must support IPAWS WEA 2.0 and IPAWS 3.0/3.1/4.0 platform, including 90 and 360 character support for WEA messages in both English and Spanish.	
8. Must support IPAWS EAS audio attachments. Describe how recordings are made and any other relevant specifications.	
9. IPAWS EAS audio should support both text-to- speech as well as recorded audio messages.	
10. Must support targeting of landline devices associated with jurisdiction addresses utilizing ANI- ALI, MSAG or GIS data sources.	
11. Describe options for sourcing community contact data from various sources.	
12. Must import geographic shape files via standard .KML files	
13. Must have the ability to store a library of reusable shapes for instant selection during activation.	
14. Must have the ability to restrict access to map areas and shapes to specific activators selectively.	
15. Must support standard drawing features within user interfaces, including polygon shapes, radius, and other options as appropriate (zoom features, different map overlays, undo, etc.). Describe interface features. Provide screenshots if possible.	
16. Must support the ability to send alerts to geographically selected users as well as other logical delivery groups.	
17. Must support scheduled notifications.	
18. Must support recurring scheduled notifications.	

19. Must support the ability to send to recipients based on real-time location. Describe capabilities and requirements.	
20. Must provide the ability to send any number of follow-up messages using the same geographic targets without requiring additional recipient selections.	
21. Must provide the ability to configure the onset and duration of geographic alerts so that they remain active as long as needed for a specific event. Describe what happens when users enter or leave a geographically-targeted notification area.	
22. Must have the ability to geographically target address-based contacts in addition to 9-1-1 data used for notifications, including residents/citizens via self-service portals, agencies, mobile applications, IPAWS and/or others.	
23. Vendor solution must have the ability to target weather notifications based on the **predicted path** of severe weather events, and to notify only residents within our jurisdiction (and/or opt-in weather notification recipients) found within the path of severe weather. Note any additional costs for weather notification functionality.	
24. Must have the ability to target mobile application users with real-time location services to determine current proximity to events and notifications.	
25. Vendor solution must provide the user with options to control participation in location-based notifications. Summarize how vendor solution ensures that citizens and residents control when and how their location is used by [JURISDICTION].	
26. Must provide functionality to notify executive staff or other key responders of the details of an ongoing messaging campaign.	

Functionality for Message Recipients	
27. Vendor solution must provide a polling capability that is "location-aware" so that user responses are returned with the current location of the responder. Use cases may include check-ins, reunification, shift or staffing opt-in, etc.	
28. Polling capabilities must not require a mobile app.	
29. Polling capabilities must provide a method for "quota notifications" that solicit availability for specific assignments and staffing needs.	
30. Quota polls must close a poll and notify the responder that a required number of responses has been met successfully.	
31. Vendor solution must support recurring polls that are sent via automation.	
32. Vendor solution must provide the ability to send targeted follow-up messages to subscribers who return a specific response in a poll campaign and/or who did NOT respond to a poll.	
33. Vendor solution must provide control over the duration of a poll.	
34. Poll responses must be available via Text/SMS, email or voice response. Note any other methods supported.	
35. Polls must have the ability to **request**, **not request**, or **require** user location with responses.	
36. Polling capabilities should be supported on the widest range of devices. Describe options as well as system requirements or apps required to collect responses.	
37. Polls must support questions and responses in multiple languages. List available languages.	

38. Polls must be able to display different content to the responder based on their selection of an answer choice.	
39. Polls must persist user response page for each subscriber showing the date and time of their response.	
40. System must support a multiple views within response reporting including: • Map view of where responses originated • List of responses as text choices • Chart or graph views of responses • Exportable response reports (specify available formats)	
41. Mobile applications must support location-based weather notifications based on proximity.	
42. Mobile applications should function outside jurisdiction. Describe capabilities.	

6. Mobile Applications and Location-Based Messaging

Requirement	Response
1. Vendor solution must offer a mobile application with substantial functionality and ease of use to members of the public. Provide an overview of mobile application(s).	
2. Vendor solution must support both Android and iOS mobile operating systems. Please specify any version dependencies or device-specific functionality, required add-on technology such as plug-ins if any, and provide a matrix of supported technology platforms and versions.	

A list of desired mobile application features follows. Please indicate whether such a feature is supported and describe functionality:	
3. Vendor solution must have the ability for residents of [Houston County, GA] communities to opt-in to receive notifications.	
4. Residents must be able to subscribe to specific sub-categories of notifications within the mobile application.	
5. Residents must be able to select which devices are utilized for each alert category and sub-category.	
6. Vendor solution must allow residents to opt-in to surrounding jurisdictional community notifications where applicable.	
7. Mobile application must support a rich profile for all members of a given household. Each member must be able to register multiple devices and contacts.	
8. Mobile application must recognize a household profile and assign a primary user for each installation of the mobile app.	
9. If your application displays a Privacy Policy or Terms and Conditions required for usage, please provide examples. Links are permitted.	
10. Mobile application must be provided free-of-charge to members of the public, including download fees as well as in-app purchases.	
11. Mobile application must not contain advertisements or third-party marketing links within the application.	
12. Mobile application user data must not be shared with any marketing or advertising concerns or utilize tracking cookies or similar functions specifically designed to enhance marketing profiles or to be shared with data aggregation services.	
13. Mobile application must provide functionality for subscribers who do not wish to provide location information for privacy reasons.	

14. Mobile application must validate registration and device information to ensure that a phone number is not only in service but also to confirm the number with a validation that confirms that the subscriber is in possession of a validated device.	
15. Web portal interoperability: Mobile application must allow the subscriber to navigate to the same information over a standard Internet browser, with all changes updated on both portal and mobile app.	
16. Mobile application must provide an informational / FAQ website to provide information to subscribers about the features and functionality of mobile application. Please provide link if applicable.	
17. Vendor must provide a support model for mobile application end users. Describe how residents receive technical support to resolve issues with the mobile application.	
18. Mobile application must provide robust accessibility features for people with disabilities and be fully compatible with mobile operating system accessibility controls and standards. Describe compliance standards and methodology.	
19. Mobile application must support [JURISDICTION}-defined categories of alert subscriptions. Within the mobile application: • A subscriber must be able to opt-in or out ofspecific notification types • A subscriber must be able to see options to selectalert groups Provide screenshots or descriptions of how resident subscribers manage household communications preferences.	
20. Mobile application must support weather notifications relevant to each user's current location, free of charge to app users, as well as a process for an end user to disable if not desired.	

21. Mobile application must be able to display “push notifications” to surface timely messages on a recipient’s device.	
22. Mobile application must support a message Inbox or similar area to display relevant and historical alert messages.	
23. Mobile application must be able to display alert notifications with rich text and media formatting.	
24. Mobile application message delivery tools must provide a means to customize the content of the push notification text separately from longer form content.	
25. Mobile application must provide robust functionality over Wi-Fi, with or without cell tower connectivity.	
26. Mobile application must support access to public notifications for area visitors.	
27. Mobile application must provide “real-time” geographically-targeted location notifications, where the system delivers messages only to mobile application users found currently within a specific geographic area.	
28. Mobile application must have functionality to send a push notification when a subscriber enters or exits the area after a message is sent.	
29. Mobile application must allow a user to browse all public notifications in a map-based interface.	
30. Mobile Application must provide a method to collect voluntary information from residents with access and functional needs and people with disabilities as part of a single registration process and workflow.	
31. Mobile application must support the ability to provide individual or household profile information directly to 9-1-1 responders.	

32. Mobile application must support the Smart911 service in use within [JURISDICTION].	
33. Mobile application must not consume excessive battery life in everyday usage to maintain reasonable battery performance with the mobile application and when using location-based services.	
34. Activators must be able to selectively include or exclude mobile application users for [Houston County, GA] alert notifications	

7. Emergency Management Decision Support

Requirement	Response
1. Vendor solution must include a secure portal for credentialed emergency management and public safety officials to access citizen/resident information voluntarily shared by subscribers. Resident information must have functions to query subscription attributes, safety and administrative question attributes, and geography based on household and business addresses. Such queries must allow emergency managers to identify: • Residents who are self-reported as having a particular accessibility need, functional need, susceptibility to a hazard, or critical dependence on a utility, service, or medical technology. • Addresses and facilities that have specific hazards, capabilities, resources, or risks. • Household members with specific needs such as residents who are non-English speakers or report dependencies on medical equipment. • Pets, livestock and other animals that may require support during an evacuation or similar emergency. • Availability as a first responder, volunteer, or agency collaborator to access [Houston County, GA] resources of value to emergency response and recovery. • Status on timely public issues such as pandemic response.	

2. Provide an overview of how the vendor solution meets these requirements.	
3. Describe how members of the public provide information to emergency management and how this information is requested.	
4. Vendor solution must provide an interfaces to query subscribers who have volunteered data.	
5. Vendor solution must allow for the export and download of citizen-supplied information in real time. List supported data export formats and reporting options.	
6. Query results produced by this solution must be closely tied to emergency notification functionality, so that a multi-modal notification can be sent to residents identified and selected by a query.	
7. Vendor solution must find subscribers who match specific query criteria and send them a two-way message or poll to confirm details or receipt of message.	
8. Vendor solution must have the ability to store pre-built queries, such that all saved query criteria can be executed against current data rapidly during critical events via current data in the system.	
9. [Houston County, GA] must have the ability to create and edit emergency notifications sent to citizens identified via a query, such that additional messaging, recipients and recipient lists, or geographies will be included in the notification.	

10. Vendor solution must support customizable roles and permissions that determine a given emergency management user's access to the system and citizen-supplied data. At a minimum, the following criteria shall be selectable at minimum: • Area (geography) of responsibility • Emergency notification delivery modes • Emergency notification distribution lists • Features/functions within Vendor's solution Describe in detail how the vendor solution addresses user roles and permissions.	

8. General Messaging

Requirement	Response
1. Vendor solution must provide the ability to initiate and deliver a notification message to all registered users on a 24/7 basis.	
2. Vendor solution should be available over standard Internet clients. List supported browsers and versions.	
3. Vendor solution must be available for alert activation on all popular smartphone and tablet operating systems.	
4. Vendor solution must support, at minimum, the following notification methods: • SMS via SMPP • Email • Outbound Dialed Voice • Social Media (Twitter, Facebook) • RSS feed (e.g., for website updates) • Common Alerting Protocol messages ○ Standards-compliant Common Alerting Protocol (CAP) message as a CAP Producer ○ Standards-compliant Common Alerting Protocol (CAP) message as a CAP Consumer • IPAWS messages for FEMA-approved alerting authorities	

○ Send messages to FEMA's IPAWS platform ○ Provide an interface to FEMA's IPAWS Labs Cloud testing platform as well as to production systems ○ Must support Required Weekly Tests (RWT) and Required Monthly Tests (RMT) • Mobile application subscribers	
5. Vendor solution must support two-way messaging. List delivery mode options supporting two-way communications and/or recipient responses.	
6. Vendor solution must provide an interactive capability by including provisions for touch-tone responses to voice notifications upon request.	
7. Vendor solution must provide scalable services to message [Houston County, GA] population effectively. Provide an overview of how the vendor solution is expected to perform reliably during widespread regional events impacting many communities. How does the solution manage real-time conditions where local networks and infrastructure may be compromised or unavailable?	
8. Vendor must provide an alternate means to send emergency messages if the Internet or other networks are congested or unavailable.	
9. Vendor solution must allow for administrators to define *ad hoc*, dynamic target recipients based on query parameters within the system. Creating a new recipient group or list must not require an operation to be run in another system.	
10. Vendor solution must provide a means for [Houston County, GA] to target all landline devices within a given geographic area (utilizing 9-1-1 ANI / ALI or MSAG data or other sources). List available data sources if any.	

11. Vendor solution must provide a means to target an individual, a subset, or the entire set of contacts known to the notification platform.	
12. Vendor solution must provide a single activation workflow to support multiple-message alert campaigns, such as the ability to send a message to previously messaged users and/or other automation features.	
13. Vendor solution must support the ability to activate multiple notifications within a notification campaign, via a single activation workflow.	
14. Vendor solution must support a function to send a message to recipients who have responded and/or to select non-respondents within a single workflow.	
15. Vendor solution must allow for the upload of a target recipient list that was extracted for another system.	
16. Vendor solution should provide functionality to ensure that content in templates is not sent without first updating placeholder text with proper values.	
17. Vendor solution must allow the creation, saving and editing of “canned” alerts.	
18. Vendor solution must allow users to set their own communication preferences (e.g., email and SMS, no email, etc.).	
19. Vendor solution must allow users to opt-out of all text messaging to a device.	
20. Vendor solution must support the use of rich text, images and access to other content and resources in email messages.	

21. Vendor solution must support file attachments to email messages.	
22. Vendor solution must ensure file attachments do not tax storage capacities and/or impact delivery performance.	
23. Vendor solution must support automated insertion of customized email headers and footers, as well as logos and other images, hypertext links, and more.	
24. Vendor solution must support configurable email branding for multiple brands. For example, the ability to support individual department, sender name, reply mailboxes, and customized header and/or footers for messages.	
25. Vendor solution must be able to detect and redial busy, no-answer, and operator intercept telephone numbers in reporting.	
26. Vendor solution must allow for configurable CallerID for voice alerting.	
27. Vendor solution must allow for a prerecorded message to precede voice alerts in order to introduce an alert available for both text-to-speech and live recorded message.	
28. Vendor solution must provide automated language translations for Text-to-Speech as well as *ad hoc* recorded voice messages in multiple languages. List supported languages.	
29. Vendor solution must allow [Houston County, GA] to configure the number of voice message replays for each alert.	
30. Vendor solution must provide a secure method to record a voice message with a single click, such that an authenticated activator is not prompted to key in user-ids, passwords, or message codes.	

31. Vendor solution must support text-to-speech (TTS) generation of voice alerts. Solution must provide a secure means in which to preview the resulting translation with a single click, such that the activator is not prompted to key in user-ids, passwords, or message codes.	
32. Vendor solution must provide a configurable voice pronunciation lexicon that can be fine-tuned by a [Houston County, GA] administrator, without vendor intervention.	
33. Vendor solution must provide a means to prompt user to create recorded messages.	
34. Vendor solution must be able to redirect return calls to a voice message hosted on the vendor platform.	
35. Vendor solution must provide an option to configure a hotline number that can be used to provide timely information to subscribers and the public at large.	
36. Vendor solution must support RSS to provide message content to web sites, RSS readers, or other RSS-enabled clients.	
37. Vendor solution must provide a method for publishing alerts via Common Alerting Protocol (CAP). The Vendor solution should support delivery of CAP documents via web-services or published to a directory as an XML document. • What versions of the CAP standard does your platform support? • What are the maximum number of CAP endpoints? • Describe mechanisms to control access to CAP capabilities.	
38. Vendor solution shall measure and adjust for network congestion or over-subscription during emergency conditions.	

39. Vendor must be able to send text messages to 200,000 subscribers within an hour. What is the SMS delivery rate capability? Provide examples of high-volume throughput / SMS delivery metrics observed in actual use of your system. Please identify the event, users targeted, and overall delivery performance.	
40. Vendor solution must support rapid delivery of voice messages. What is the delivery rate capability?	
41. Vendor solution must allow for organization-defined active call throttling configuration to reduce the chances of congestion and subsequent call retries for voice alerts to organization facilities.	
42. Vendor solution must support multiple call throttling rules, with each rule defining a concurrent call limit to be applied on an unrestricted number of [JURISDICTION]-defined numbers and locations.	
43. Vendor solution shall automatically measure and adjust for voice network congestion, reactively adjusting calls when downstream network capacity has exceeded call throughput.	
44. Provide an overview of the vendor solution's reporting and analytics capabilities.	
45. Vendor solution shall provide a comprehensive voice call, SMS and email reporting capability.	
46. Vendor must provide reports with substantial and transparent detail to analyze messaging to the individual recipient level across all personal delivery modes.	
47. Vendor solution must work across all major wireless carriers and wireless phone models. Describe any limitations and how the system addresses delivery to smaller carriers. How many carriers are supported? How does the vendor manage changes to the industry landscape among mobile and landline carriers?	

48. Vendor must demonstrate an effective SMS delivery architecture. Describe your SMS delivery architecture. Do you deliver messages via SMTP or SMPP? If delivery is via SMTP only, please detail carrier whitelisting relationships. If SMPP, does your system utilized direct binds, aggregators or other middleware providers? What safeguards are in place to ensure message delivery?	
49. Vendor solution must allow {JURISDICTION] to post notifications to social media feeds.	
50. Vendor solution must provide access controls to protect social media accounts among multiple [Houston County, GA] system stakeholders sharing a system with multiple social media accounts.	
51. Vendor solution must allow [JURISDICTION]'s alert activators to specify a single set of message content, and automatically deliver the common message content across all notification methods.	
52. Vendor solution must support scenarios where multiple notifications may be sent via a single activation with flexible capabilities such as rules, conditional actions, automation options, or other features specific to management of complex notification scenarios.	

9. Internal Employee, Staff and Operational User Messaging

1. Vendor solution must provide robust features supporting staff notifications.	
2. Vendor solution must manage user account and contact data for internal (employee/staff) users, entirely separated from public subscribers.	

3. How does the vendor solution manage groups? Provide an overview of group and sub-group management functionality.	
4. Vendor solution must ensure that public subscribers do not see [Houston County, GA] messaging intended for internal use only.	
5. Vendor solution must ensure that messages may selectively target specific groups of organizational internal staff, agencies, departments, and locations.	
6. Contact information and opt-in preferences for internal staff must be managed separately from citizen users. Modifications to citizen user accounts created by employee users must not affect internal notification contacts or preferences.	
7. Staff and employees with both citizen and staff accounts must not receive duplicate messages during notification campaigns.	
8. Vendor solution must provide [Houston County, GA] with the option to allow or prohibit internal users from self-managing their account through a jurisdiction-branded registration portal.	
9. Jurisdiction must have the ability to select from the following authentication methods to control access to the staff / employee user registration portal: • Authentication native to the vendor solution • Integration with [JURISDICTION]'s LDAP server • Integration with Jurisdiction's Active Directory or ADFS • Integration with Jurisdiction's CAS or Shibboleth SSO • Integration with Jurisdiction's SAML2-based SSO • Authentication support for enterprise platforms such as Azure, Okta or others.	

10. Vendor solution must provide administrative access to send alerts in the event that enterprise authentication systems are under maintenance or otherwise unavailable.	
11. [Houston County, GA] staff users must be able to opt-in or be assigned to recipient group affiliations.	
12. Vendor solution should allow administrators to create their own groups.	
13. Vendor solution should allow administrators to create their own groups within a [Houston County, GA] defined delegated administration capability that pushes access permissions to sub-group administrators.	
14. Vendor solution must enable [Houston County, GA] staff to subscribe to message categories via SMS as well as within self-service portals, and to prevent external subscribers from subscribing to internal organizational groups by configuration.	
15. Describe any features designed to support messaging to visitors, guests, and temporary, part-time or contract employees.	
16. Vendor solution must allow administrators to define groups as “private” (visible only to authorized users) or “public” (visible to subscribers with access to self-service portals or subscribers using a text-message opt-in method).	
17. List any additional costs or other limitations on messaging and usage for internal and operational notifications. Where relevant, specify additional licensing and cost impact of this functionality.	

10. User Management

Requirement	Response
1. Vendor solution must validate that a subscriber who registers provides a valid contact, and for mobile and landline phone contacts is in possession of the registered device.	
2. Vendor solution must allow for regular automated refreshes of user contacts captured outside the vendor system, e.g, from enterprise ERP/HR system resources.	
3. Vendor solution must allow for regular updates of user-to-group associations to facilitate targeted messaging.	
4. Vendor solution must permit/restrict activator permissions to message defined groups that are a subset of the larger user population. Higher level administrators must be able to define those permissions in a secure manner.	
5. Vendor solution must provide a user interface for administrators to manage user information within the system.	
6. Vendor solution must ensure that only specific administrators may edit or access user data based on permissions.	
7. Vendor solution should provide a view for help desk staff to manage subscriber information without the ability to send notifications.	
8. Vendor solution must support custom fields tied to tags or data attributes specific for each user, in order to define dynamic selections of alert recipients based on current data. List the number of custom fields available if any.	
9. Describe the processes recommended for administering the system and authorizing users to generate messages and broadcast alerts.	

10. Vendor solution must provide transparent reporting and analytics tools that detail the integrity of the contact information in the system. Examples include reports of undeliverable emails or contacts, solution usage reports, and post-messaging reporting.	
11. Vendor solution must allow user registration via SMS. Solution must have a mechanism for authenticating, suspending, and removing those subscribers.	
12. Vendor solution must provide a branded self-service web site where registered staff can modify their contact information and preferences.	
13. Vendor solution must have the ability to generate a dynamic distribution list based on data queries of residents matching certain search criteria, such as access and functional needs, people with disabilities, people in care facilities, people with language or other communications challenges when contacting emergency responders, or other descriptive properties necessary for inclusive emergency management programs.	
14. Describe any additional costs or other limitations on messaging and usage for internal and operational notifications.	

11. Safety Responder Collaboration, Coordination and Event Communications

Requirement	Response
1. Vendor solution must include features that support collaboration, focused on tactical collaboration among interdisciplinary teams around a specific series of actions, scenarios, and automated actions. For example, a message may initiate a series of actions performed by multiple responder groups.	

2. Vendor solution must manage task assignments, process documentation, and resources relevant to specific disciplines such as safety / security staff, HR, facilities, emergency management, executive staff, PIOsa, operations, etc. Participation and tasks must be configurable by event type.	
3. Vendor solution must notify all collaborators via multiple mechanisms (e.g., text, voice, email, or push notifications to a mobile application).	
4. List system requirements or applications required for team members to use this functionality. List compatible operating systems or other installed components.	
5. Vendor solution must provide incident-specific communications among solution administrators, defined responder groups, initiated via automated or manual response initiation. Examples include severe weather events, active assailant scenarios, and civil and location-based risk events.	
6. Vendor solution must initiate a scenario when specific messages or templates are activated.	
7. Vendor solution must support recurring tasks performed during an incident.	
8. Vendor solution must support *ad hoc* creation, assignment, and management of tasks and responder assignments during an incident in response to changing conditions.	
9. Vendor solution must provide all collaborators visibility into overall incident activity and status.	
10. Vendor solution must support a rapid method to connect responders with an incident-focused conference bridge.	
11. Vendor solution must provide an audit trail for response activity via after-action reporting.	

12. Vendor solution must support a library of documents and other response plans for collaborators during the incident. These plans must be supported in real-time.	
13. Vendor solution must provide a simple mechanism to enable rapid notifications during an incident and ensure that notifications are included in audit reporting.	
14. Vendor solution must provide visual status information during an active incident.	
15. Vendor solution must support the ability to automate additional notifications when a scenario is initiated.	
16. Vendor solution must be able to restrict authorizations for initiating and completing an incident.	
17. Vendor solution must support options to manage and log recurring drills, exercises, inspections, or other safety compliance activities required for routine assignments.	
18. Note any additional licensing and/or costs for incident management functionality where applicable.	

12. Integrations and Partner Ecosystem

Requirement	Response
1. Provide an overview of the vendor firm's available strategic, technology or other business partnerships, highlighting integrations and interoperability relevant to the proposed solution.	
2. Vendor solution must provide application programming interfaces (APIs) that will facilitate automated messaging through the system's message delivery architecture from [Houston County, GA] bespoke technology platforms.	

3. Vendor solution must expose API's for the purpose of user management functions such as creating user accounts, subscription affiliations, custom data fields,	
4. Vendor solution must provide features supporting Houston County 911 center.	
5. Vendor solution must be integrated with the Smart911 system.	
6. Vendor solution must accept standards-compliant CAP messages from external systems to trigger a multi-modal broadcast alert and to activate other remote systems compatible with this standard.	
7. Vendor solution must natively integrate with the Juvare WebEOC incident management platform: a. Vendor solution should be able to associate multiple messages with a single Juvare WebEOC incident board for timely and after-action reporting purposes. b. Vendor solution should be able to construct messages via automation using information managed in the Juvare WebEOC incident board. Describe functionality. c. Vendor solution should display incident-related messaging reports within an incident board managed within the Juvare WebEOC platform.	
8. List any additional partnerships and integration points specifically relevant to the requirements presented in this bid. These may include other notification systems, technology, information security and business continuity partners, system integrators, purchasing vehicles, access controls systems, or risk management systems.	

13. Implementation, Training and Support

Requirement	Response
1. Provide an overview of the implementation process for the vendor solution.	
2. Vendor solution must provide materials, supporting content and templates, or best-practice communications tools to maximize service adoption and registrations for both public and internal staff subscribers. Note any additional licensing or costs if any.	
3. Vendor solution must provide initial training for system administrators and operators. Note all licensing and training costs for training.	
4. Vendor solution must make training materials available 24/7 to support shift workers unavailable during daytime business hours.	
5. Vendor solution should provide a training certification program to track staff training and compliance.	
6. Provide a brief description of the major steps in the implementation process, including IT or other jurisdictional /agency / system stakeholder resource requirements.	
7. Must support geographically dispersed solution stakeholders working remotely during implementation and during events such as pandemic lockdowns in 2020-21. Note any requirements for onsite presence during implementation.	
8. Provide onboarding timelines, milestones, project phases and project plans for implementing the system during [Houston County, GA] onboarding.	

9. Vendor must provide 24/7/365 phone support. Describe the support levels and service levels.	
10. Vendor must provide 24/7 access to support ticketing systems used to track both open and completed support incidents.	
11. Provide the vendor's Service Level Agreements (SLA) and standard contracting vehicle(s) in an appendix to this response.	
12. Vendor must provide robust technical support services. Note any limitations, additional licensing, or services costs for administrator access to technical support.	
13. List any ongoing resource requirements expected from [Houston County, GA] after completion of onboarding.	
14. Provide a proposed project plan used in onboarding. If available, please provide a table outlining project details, phases and milestones.	
15. Vendor must provide robust support after conclusion of onboarding activities and production launch of solution.	

14. Product Roadmap, Other Capabilities and Future Enhancements

Requirement	Response
1. Vendor must provide a means to request enhanced functionality. How are solution enhancements prioritized and released?	
2. Vendor solution upgrades must not disrupt system usage. Note how often system upgrades are performed, how is the [Houston County, GA] notified of changes, and when release details are available for in advance of release.	

3. Vendor must provide regular updates on new and improved functionality added to the system.	
4. Provide a brief overview of the general direction of your development focus and solution roadmap over the next year and how you feel these may impact the [JURISDICTION]'s required capabilities.	
5. Provide a general summary of your Quality Assurance (QA) methodologies and release processes.	
6. Describe any available options to support chat or tip reporting for either public users, internal staff, or other jurisdictional stakeholder communications.	
7. Describe any user groups, conferences, online forums, or other customer support options available during the duration of vendor contracting both before and after initial onboarding.	

15. Information Security and Data Privacy

Requirement	Response
1. Provide or append an overview of Vendor's overall approach to Information Security best practices.	
2. List all relevant information security certifications supported by the solution platform (e.g., Cloud Security Alliance (CSA), NIST/ISO certifications, FedRAMP, Safety Act, etc.).	
3. Vendor must maintain a documented information security policy and security awareness program for all vendor staff with access to [Houston County, GA] data?	
4. Vendor solution must store data within the United States. Data must not be stored on systems residing outside the US.	

5. Detail which vendor staff will have access to [Houston County, GA] data and how access is audited.	
6. Provide the location of vendor data center(s) that will be used to provide this solution.	
7. Vendor solution and platform must have undergone a SSAE-18 audit. Provide SOC2 Type 2 (preferred) or SOC3 reports with this response.	
8. Vendor staff must be required to complete mandatory security compliance and awareness training for all vendor staff. Note how staff compliance training is administered and required re-certification requirements.	
9. Vendor organization must have physical security controls and policies in place and enforced.	
10. Vendor must provide 99.999% service availability.	
11. Vendor should provide any application data Privacy Policies and/or Terms and Conditions presented to service subscribers. Links are acceptable.	
12. Vendor must perform regular Penetration Testing. How often are these performed?	
13. Provide documentation of penetration test results, high/medium/low risks identified, and how they are mitigated.	
14. Has the Vendor had a significant data breach within the last 5 years? If so, describe.	
15. Vendor must notify [Houston County, GA] stakeholders in the event of a data breach. Note method(s) of informing stakeholder organizations in the event of a data breach.	

16. Vendor solution must support two-factor or multi factor (2FA/MFA) authentication security.	
17. Vendor must demonstrate an adequate Business Continuity and Disaster Recovery plan and should discuss the methods and hosting infrastructure in place to ensure system redundancy. • If available, provide vendor Business Continuity Plan (BCP) documentation. How often is this plan reviewed and updated? • If available, provide vendor Disaster Recovery Plan (DR) documentation. How often is this plan reviewed and updated?	
18. Vendor solution must test its disaster recovery capabilities regularly. Provide frequency of planned DR testing and date of last DR exercise. Where available, Recovery Point Objective (RPO), Recovery Time Objective (RTO), and other relevant components of the vendor's disaster recovery strategy.	
19. Will any subcontractors or other outside services staff have access to [Houston County, GA] data. If so, describe how the subcontractor(s) are vetted.	
20. All [Houston County, GA] data must be stored in encrypted format both ***in transit*** and ***at rest***. Specify encryption standards.	
21. Is any [Houston County, GA] data used for notifications dependent on third-party or contracted cloud infrastructure platforms (e.g., AWS, Azure, etc.)? If so, describe any redundancies in place to cover the event of a services outage.	

22. How does Vendor platform protect [Houston County, GA] data from Distributed Denial or Service (DDoS) or similar attacks?	
23. Vendor must monitor all platform systems on a 24x7x365 basis? Describe policies, procedures and/or relevant tools in use.	
24. Is intrusion monitoring performed internally or by a 3rd party service? Note any relevant tools in use.	
25. Vendor solution must be developed with strict secure coding practices. Note standards such as CERT, OWASP, etc. supporting development and operations teams.	
26. Vendor solution must implement tools to scan for vulnerabilities in all applications and platform systems.	
27. Vendor must monitor for and protect against common web application security vulnerabilities, such as SQL injection attacks, XSS, XSRF, and similar exploits.	
28. Vendor platform must utilize firewall technology such as a stateful packet inspection firewall.	
29. Vendor must utilize Intrusion Detection (IDS) and Intrusion Prevention (IPS) systems. Note platform and/or configuration tools in use.	
30. Vendor must utilize host-based intrusion systems to monitor intrusions on a 24/7 basis. Note whether intrusion monitoring is vendor-maintained or a performed by a third-party service.	
31. List documented data classification policies related to access of [Houston County, GA] data.	

32. Are there any single points of failure in messaging delivery infrastructure? How are connections between your hosting centers and “last mile” infrastructure (e.g. calling centers, SMS aggregator binds, email servers, etc.) configured to minimize delivery faults along the message delivery pipeline for the various message types.	
33. Vendor must provide security for individual data. Describe your policies for ensuring data privacy and security.	
34. Vendor must confirm that subscriber information will not be used for advertising or released to third parties not connected to the system for marketing or other purposes.	
35. Vendor solution must provide a completed Cloud Security Alliance (CSA) CAIQ assessment for information security. Attach documentation to this response.	
36. Vendor must demonstrate regular, third-party auditing and review of all security procedures.	
37. Vendor must have a dedicated Information Security staff. If so, provide title of functional manager of this function and reporting structure.	
38. Vendor should describe its data back-up and recovery policies. Backups must be encrypted; what type of encryption is used?	
39. Describe all relevant employment practices regarding information security, for example: • Who maintains primary responsibility for platform security (roles) and employee access to [Houston County, GA] data? • Employee screening and monitoring programs • Required security training programs for new and continuing staff • Exit procedures for staff separating from the organization.	

• Ongoing review of operational security measures and employee compliance programs.	
40. Vendor solution must work across all major wireless carrier networks and wireless phone models. Describe any limitations and how the system addresses delivery to smaller carriers.	
41. Vendor systems must prevent unauthorized physical contact with solution architecture.	
42. Vendor solution must perform scheduled and encrypted backups of subscriber data. Note the vendor's records-retention policy.	
43. Vendor have a documented process for operational configuration and patch management.	
44. Vendor must be certified for FedRAMP compliance.	

Pricing

Illustrate all financial elements in this Section so that all costs (one-time, fixed, recurring, ongoing, optional, usage based, etc.) for all services, hardware, software, licensing, hardware maintenance, software maintenance, development, documentation, training, support, and operation are reflected. All pricing should be broken out by line item category. The Vendor shall also list and price any item that is part of the solution (whether hardware, software, or management-related) that has not been specified in the requirements but is needed in order for successful installation, development, and operation of this service.