



# Southeast Texas Regional Technology Governance

**Houston UASI Technology Work Group**  
May 2020



# Table of Contents

I. Purpose Statement .....	1
II. Work Group Structure.....	1
III. Roles and Responsibilities .....	2
IV. Recommendation Review Process .....	3
New Technology Suitability .....	4
V. Regional Technology and Contracting Standards.....	5
Project Requirements .....	5
Deliverable Requirements.....	6
Security and Resilience Requirements.....	6
Reporting .....	8
Training and Exercises .....	8
Licensing and Contracts .....	9
Compliance with Governance .....	9
VI. Regional Technology Systems .....	9
Regional Crisis Information System .....	10
Regional Emergency Public Information System .....	11
Regional Emergency Notification and Warning System .....	11
Regional Resource Cataloging and Badging System .....	12
Regional Geographic Information Systems Server .....	12
Regional Video Conferencing System.....	12
VII. Revisions.....	13
VIII. List of Acronyms .....	13



## **I. Purpose Statement**

The Houston Urban Area Security Initiative (UASI) Technology Governance Document is intended to:

- guide the UASI Executive Committee and Regional Collaboration Committee on regional technology;
- help with writing strategic information technology recommendations;
- set directions and priorities for regional information technology resource allocations;
- contain standardized procedures related to the use of regional information technology;
- establish a mechanism for overseeing and evaluating the overall performance and management of the UASI-funded information technology systems;
- serve as a framework for the operation of the Regional Collaboration Committee's Technology Work Group and sub-work groups;
- document how regional technology is used to satisfy the Houston Urban Area Homeland Security Strategic Plan;
- unify the approach to administration of technologies funded by the Houston UASI grant program; and
- simplify the adoption of new technology.

This document only covers technologies that were recommend for funding through the Regional Collaboration Committee. Other UASI committees may recommend the funding of technology (software and hardware) not covered in this document. In addition, the UASI Executive Committee may allocate funding to a jurisdiction for a technology project that is not regional in scope. Because of this, the requirements in this document do not apply to other committees' technologies or to non-regional technologies. However, other committees and individual jurisdictions are encouraged to use this document as guidance when developing their own governance.

## **II. Work Group Structure**

The Houston UASI Executive Committee comprises four members representing the City of Houston and the counties of Fort Bend, Harris, and Montgomery. The Executive Committee holds regular meetings to vote on issues affecting the grant program, including final approval of funded projects. Under the Executive Committee are multiple standing committees,

which also hold regular meetings, and vote on issues related to their area of responsibility. This includes preliminary scoring of potential grant-funded projects for the coming fiscal year. The Regional Collaboration Committee, as a standing committee, has the authority to set up work groups as needed. This includes the Technology Work Group and any sub-work groups specific to a certain technology.

The Technology Work Group is a consensus body. Any key decisions made by the Work Group will be submitted as recommendations to the Regional Collaboration Committee for review. The Committee can vote to act on recommendations from the Work Group.

Technology Work Group meetings are open to regional partners. Each meeting includes time for vendors to present on their products with the approval of the co-chairs; however, vendors may not attend portions of the meeting where the work group discusses other technology systems. Partners wishing to be added to the meeting notification list should contact a co-chair using the contact information listed on the Houston UASI website.

The Technology Work Group will have two co-chairs who are approved by the Regional Collaboration Committee. Their role will be to run meetings, keep meeting agendas and minutes, manage any of the group's collaborative efforts, such as authoring reports, and represent the Work Group during committee meetings. There is no set term, and any change in co-chairs must be submitted to the Regional Collaboration Committee per its guidelines.

### **III. Roles and Responsibilities**

The Technology Work Group and its sub-work groups are responsible for implementing direction and priorities for development of the technological resources as set by the Regional Collaboration Committee. Additionally, the work groups are encouraged to collaboratively resolve any issue related to problems or enhancement requests assigned by the Committee and share recommendations for review.

The Technology Work Group reviews and analyzes technology to satisfy the UASI Strategic Plan. After the region finishes each new version of the UASI Strategic Plan, the Work Group will meet to compare the gaps in the Houston Urban Area Homeland Security Strategic Plan with existing regional technologies. In addition, the Technology Work Group serves as a hub for all

system administrators to meet and discuss topics that affect multiple technologies already used by the Houston UASI or any regional technology which does not have its own work group. This document directs the Technology Work Group in these tasks. The Regional Collaboration Committee may assign added tasks and provide additional guidance, as needed.

If an existing regional technology does not have a designated system administrator (due to a vacancy in the position), the jurisdiction employing the previous administrator will appoint an acting administrator. If the jurisdiction does not appoint an administrator, the Regional Collaboration Committee may direct the Technology Work Group and/or a dedicated sub-work group to assume the various administrative tasks for that technology. Throughout this document, the term "system administrator" will mean the acting administrator, Technology Work Group, or a dedicated sub-work group if there is not a system administrator.

#### **IV. Recommendation Review Process**

The Technology Work Group may recommend changes or additions to the regional suite of technology based on recent developments (e.g. technological, strategic, emergency management practices). Technological subject-matter experts on the Work Group can review and make recommendations for new technology to help determine the feasibility of the technology as a regional solution.

The following process is used if a regional partner requests that the Technology Work Group make a recommendation to the Regional Collaboration Committee, including cases where a new regional technology or a change in an existing regional technology is proposed.

1. A regional partner makes a written request to the Technology Work Group co-chairs, documenting the recommendation along with relevant background information.
2. The Work Group co-chairs will add discussion of the recommendation to the agenda of the next practical meeting, and a copy of the proposal will be sent to the Technology Work Group distribution list for review prior to the meeting.
3. The participants at the meeting will discuss the recommendation and, if necessary, make revisions.

4. The Technology Work Group co-chairs will use the revised recommendation to draft a formal recommendation.
5. The co-chairs will send the formal recommendation to the Technology Work Group distribution list no later than two weeks before the next Technology Work Group meeting for advance review.
6. The Technology Work Group will review the formal recommendation, and if the group reaches a consensus, the co-chairs will send the recommendation to the Committee.
7. If the work group does not reach consensus on a formal recommendation, the Technology Work Group may choose to extend the discussion period into future meetings, or the co-chairs may make multiple recommendations to the Committee.

The Technology Work Group follows a similar process when producing and approving other requested documents and reports.

### ***New Technology Suitability***

Any new regional technology projects recommended by the Technology Work Group must address a gap from the current UASI Strategic Plan. The Work Group will help the requestor find potential technology solutions that bridge the gap and adhere to regional technology standards described in this document. This process must include a review of multiple available options and documentation of why certain options are preferred over others. The outcome of that process will be a change request or project proposal, which must then be shared with the Technology Work Group via the recommendation review process described previously.

During each regularly scheduled meeting, the Technology Work Group will reserve time for presentations on new use cases for existing regional technology or new technology that can bridge strategy gaps. In addition, one Technology Work Group meeting per year (as determined by that year's UASI grant schedule) will be an open forum to hear presentations on regional technology that can bridge strategy gaps. Invitations to this meeting will be sent out to all members of the Regional Collaboration Committee and all regional system administrators. It is the responsibility of jurisdictional emergency management partners to share this information within their jurisdiction and with other jurisdictions they interact with as appropriate.

To allow enough time for the recommendation review process on items which affect future grant-funded project applications, the Technology Work Group encourages gap presentations be made at least three months before the expected committee application scoring meetings to allow for thorough consideration and review. A similar time frame should be anticipated for recommendations requested on other topics.

## **V. Regional Technology and Contracting Standards**

The following standards apply to all regional technologies. In addition to these standards, individual regional technologies may have their own policies, procedures, workflows, job aids, and training guidance. It is the responsibility of each technology's system administrator to develop and maintain these items as appropriate. Each regional technology's associated documents will be maintained on the Houston UASI website in the same location as this governance document.

### ***Project Requirements***

The following apply to both new projects and enhancements that are under the purview of the Technology Work Group. The purchasing and project management process will be the responsibility of the jurisdiction responsible for the UASI project and governed by that jurisdiction's policies and procedures. However, the guidelines in this document should be respected to the greatest extent possible.

Each vendor will propose a scope of work document that describes the work they will complete, planning milestones, and deadlines. This document must include a meeting schedule and intended audience and the relevant system administrator must approved it. It is the system administrator's responsibility to coordinate with their jurisdiction's purchasing authorities to ensure that the scope of work document and related materials are in order. The relevant system administrator should brief on the scope of work document at the first practical Technology Work Group meeting and share the document on the UASI website for regional situational awareness.

The Technology Work Group is available to help the jurisdiction develop a detailed scope of work or other procurement guidance that meets the standards set out in this document and appropriately considers the UASI strategy.

It is the responsibility of the system administrator and their jurisdiction's purchasing authority to adhere to policies about preferential business groups and all grant guidance and regulations. These considerations should be made at the start of the purchasing process.

### ***Deliverable Requirements***

When performing custom work (not using a commercial off-the-shelf product), anyone performing work must use a standards-based approach. Those standards, specified by the vendor and/or the Technology Work Group, must maximize accessibility by persons with access and functional needs; compatibility with various devices, platforms, and browsers; integration with other technologies and systems; and longevity of the product to avoid unnecessary obsolescence.

When anyone performs work on an existing system that will severely reduce its functionality for the Houston UASI region, they must notify all relevant system administrators before performing the work. This notification must be delivered in writing at least seven days prior to the scheduled downtime or period of reduced service. It is the responsibility of the relevant system administrator to notify the Technology Work Group and applicable users.

Any deliverables produced by a vendor specifically for the Houston UASI region, including customized training programs, job aids, and customized modules or components are the property of the Houston UASI, and their use and dissemination are at the discretion of the Regional Collaboration and Executive Committees.

### ***Security and Resilience Requirements***

It is everyone's responsibility to take reasonable steps to protect regional technology from intrusion or abuse. User access levels must be clearly defined and communicated, and training should be developed for each access level. Each regional system must have the following minimum standard user groups and training programs, with more granularity allowed on a technology-by-technology basis:

1. Regional Administrator
2. Power User
3. User

Each user account must correspond to an individual so that actions taken in

the system can be traced back to the user. The use of “multiuser” accounts (i.e., a single account that is accessible by multiple individuals with no tracking of which person performed a particular action) in any regional system is to be restricted to limited testing purposes only. Once such accounts are no longer in use, they must be removed or deactivated.

The Technology Work Group expects vendors to conduct regular security audits on their systems and to share the overall findings of those audits with the system administrator. System administrators should report to the Technology Work Group when audits have been conducted on their technologies or if they are notified by the vendor of any security irregularities. If the Technology Work Group determines that a technology has a security deficiency that could prevent its use, the work group co-chairs will notify the Regional Collaboration Committee Chair and Vice-Chair, and the system administrator will work with their jurisdiction’s purchasing and legal departments to determine a course of action. The system administrator and/or the Committee Chair and Vice-Chair (in consultation with the Technology Work Group) will decide if the issue calls for a temporary suspension of use of the affected technology.

The system administrator will perform user audits quarterly, at a minimum, and any inactive users will be removed from the system. The process for performing an audit differs between technologies, but after the system administrator performs the audit, they must send an audit summary to the Technology Work Group. January, April, July, and October Technology Work Group Meeting agendas will include an agenda item for system administrators to verify that their user audits have been conducted.

Jurisdictions must collaborate with the relevant system administrators regarding staffing changes that affect user accounts, particularly those with elevated permissions. Jurisdictions should notify administrators when staff who held accounts with elevated permissions leave an organization, and the relevant system administrator should take the necessary steps to disable those accounts promptly. The jurisdiction should then coordinate with the relevant system administrator (and any applicable committees or work groups) on appointing a replacement jurisdictional representative with elevated permissions and ensuring that the replacement receives any necessary training.

Any web-hosted technology must have fully adopted the ISO/IEC 27001 standard and have reviewable security policies based on ISO/IEC 27002. It is acceptable for software providers or hosting companies to require the signing of non-disclosure agreements prior to sharing security policies.

Connections with web-hosted technology must be encrypted using Secure Socket Layer or Transport Layer Security protocols from point to point. Passwords and other sensitive information must be hashed and salted, not stored in plain or encrypted text.

### ***Reporting***

System administrators should track usage of their systems and brief out about technology use and adoption at the Technology Work Group meetings. Administrators should be prepared to share a roll-up report at committee application review meetings for a system with a sustainment or enhancement grant application.

At a minimum, reports should include updates on outstanding technical issues, information on software version changes and summaries, and summaries of changes to current use (number of users, number of active users, and/or number of participating jurisdictions).

### ***Training and Exercises***

The region will develop training programs for the use of any regional technology within two years of its adoption. The relevant system administrator creates, delivers, and maintains training programs. The Regional Multi-Year Training and Exercise Plan will include a system training schedule each year, and the individual technology's system administrator is responsible for the maintenance and updating of the training program as needed. The system administrator will also maintain a record of trained users as appropriate for their system.

The Technology Work Group will maintain a section on HoustonUASI.com titled "Regional Technology," where use of each regional technology will be advertised. The section will publicly list each regional technology with a description of its use, a link to its logon page (if applicable), a link to training materials, a link to any technology-specific documentation, and system administrator contact information.

The Work Group encourages the use of regional technologies during

exercises as practical.

### ***Licensing and Contracts***

The region gives strong preference will to software packages that offer licensing models that encourage wide adoption of the system. The region will also give preference to systems which allow individualized user accounts without restriction on the number of users or number of uses of the system within the specified contract period. In addition, the region will give preference to options that use a lifetime license with an ongoing maintenance agreement to facilitate sustainment by buying down the region's future financial obligation.

Vendors should include clear language in all contracts noting conditions under which a license can be cancelled, along with the amount of notice given to the purchasing jurisdiction prior to revocation of a license or discontinuation of a product.

Contracts should be written with a clause that says that the Houston UASI must retain rights to all data input into a technology system and must be able to retrieve said data at its discretion or if a product is discontinued. That data export should be in a machine-readable format conducive to transferring the data to a potential replacement system. Vendors should provide the requested data within timeframes set by legislation related to government records requests.

### ***Compliance with Governance***

The Technology Work Group will document any violations of this governance document and try to resolve the issue with the relevant system administrator (or that person's supervisor, if applicable). The results of this interaction will be included in the documentation of the violation. Should the administrator or their supervisor not be able to resolve the issue, all corresponding documentation, along with a recommended course of action, will be given to the Regional Collaboration Committee for debate and action.

System administrators are responsible for ensuring respective technologies follow this document's requirements and recommendations.

## **VI. Regional Technology Systems**

Each grant-funded regional technology system under the purview of the

Regional Collaboration Committee is listed below. Administrative contacts for each are shared on the Houston UASI website.

Some technologies do not fully adhere to this governance document or have expanded scope not covered in the standards above, those differences are listed under each technology section below as exceptions to governance.

### ***Regional Crisis Information System***

<b>Technology Solution Name:</b>	WebEOC
<b>Vendor:</b>	Juware
<b>Responsible Jurisdiction:</b>	City of Houston

**System Description:** WebEOC is an online system for sharing information and resource requests via forms and dynamic displays (called boards) within and between emergency operations centers. WebEOC was originally purchased with non-UASI funding, and as a result, has a footprint that extends outside the UASI region. WebEOC is the State of Texas' preferred crisis information system, and it is also used for other state-wide emergency management functions, such as resource requests.

**Exceptions to Governance:** WebEOC has a different hierarchy of user levels. Users are individuals who log into the system and create and share information. Each jurisdiction can be allotted one or more Sentinels, who serve as local Power Users in the system. Sentinels can create incidents, facilitate account creation via Position Access Codes (PAC), and may be responsible for end-user training. Sub-Administrators have additional permissions in the system, including the ability to create, edit, and delete users and change user positions within a specified subset of users (normally a jurisdiction or agency). The system is overseen by a Regional Administrator, who ensures that a coordinated WebEOC training program is in place, oversees the Sentinels and Sub-Administrators, and handles other administrative tasks. In addition, the grant funds a WebEOC Programmer who is responsible for maintaining, updating, and creating boards on the Southeast Texas WebEOC Server and overseeing any contract developers. The Regional Administrator and WebEOC Programmer both take direction from the WebEOC Sub-Work Group, which is a subset of the Technology Work Group under Regional Collaboration Committee.

In addition, some WebEOC accounts (specifically for evacuation use) are generic by position/role and not assigned to specific individuals. These

accounts are activated only on a short-term basis, and access is limited solely to the State of Texas Emergency Tracking Network and no other WebEOC data.

### ***Regional Emergency Public Information System***

**Technology Solution Name:** Jetty  
**Vendor:** The Response Group  
**Responsible Jurisdiction:** Fort Bend County

**System Description:** Jetty is a web-based contact, content, and inquiry management system designed for use in emergencies. The system’s features include versioning of media releases, a defined document approval process, and tracking of inquiries and responses.

**Exceptions to Governance:** Jetty calls the Regional Administrator the Network Administrator. Rather than having Power User or User roles, there are specific “Manager” and “Support” roles which have power user or user abilities over the functions they are assigned (e.g., inquiries, documents, translations).

### ***Regional Emergency Notification and Warning System***

**Technology Solution Name:** AlertFM  
**Vendor:** Global Security Systems  
**Responsible Jurisdiction:** Montgomery County

**System Description:** AlertFM includes three components:

1. A proprietary warning system that uses commercial radio station subcarrier signals to broadcast messages to AlertFM receivers.
2. A web-based Integrated Public Alert and Warning System (IPAWS) message origination portal, which allows access to Wireless Emergency Alerts (WEA), the Emergency Alert System (EAS), the AlertFM system, and other platforms.
3. A mobile phone application that can be used to send push notifications to users based on the user’s specified location.

**Exceptions to Governance:** The licensing agreement for AlertFM specifies that each participating jurisdiction gets a fixed number of user accounts to the message origination tool. Because of this, AlertFM licenses are assigned to positions rather than individual users. It is the responsibility of each participating jurisdiction to ensure account and system security and accountability with its licenses. In addition, AlertFM does not have a regional

system administrator.

### ***Regional Resource Cataloging and Badging System***

**Technology Solution Name:** i-INFO  
**Vendor:** Alliance for Community Solutions  
**Responsible Jurisdiction:** Montgomery County

**System Description:** i-INFO is an online database system used for managing material and personnel assets. Additional functions of this system also support regional scheduling of mass prophylaxis by health departments.

**Exceptions to Governance:** The user structure within i-INFO differs from the standards described in this document. Data Users are individuals who are registered individuals in the system. They can log in to update their own information only. Portal Users can manage resource and personnel information through an administrative interface. The System Administrator functions as a Regional Administrator. There is no Power User position in i-INFO.

### ***Regional Geographic Information Systems Server***

**Technology Solution Name:** Various  
**Vendor:** Esri  
**Responsible Jurisdiction:** City of Houston

**System Description:** Esri GIS software is hosted by a third-party provider and is used to facilitate sharing of geographic information throughout the region, as well as handheld devices capable of accessing and interacting with data on the server.

**Exceptions to Governance:** Because documentation for this project has not been written, no exceptions can be noted, except that the grant does not fund a Regional GIS Server Administrator. The GIS Work Group manages the use of the server, and City of Houston staff manage the project.

### ***Regional Video Teleconferencing System***

**Technology Solution Name:** Lifesize  
**Vendor:** Various  
**Responsible Jurisdiction:** Various

**System Description:** Lifesize allows sharing of voice and video feeds between locations, through proprietary hardware, software installed on

computers, and web-based systems.

**Exceptions to Governance:** While the various grant-funded video teleconferencing (VTC) systems in the region can connect with one another and were funded through a regional project, each bridge is administered by the jurisdiction that hosts it. This includes managing users on the bridge. In addition to accounts assigned to individuals, accounts can also be assigned to specific rooms/locations (e.g., a camera and phone installed in a conference room); this is an exception to the one account per individual preference.

## VII. Revisions

The Technology Work Group and its sub-work groups will review this governance document every three years or as directed by the Regional Collaboration Committee. The work group or sub-work group will review all recommendations for changes. The work group will then send these changes to the Committee for approval and subsequently the Executive Committee for final approval.

In the event a technology's system administrator or sub-work group wants to revise their section of the governance outside of the scheduled review period, they will follow the Recommendation Review Process outlined above

## VIII. List of Acronyms

EAS	Emergency Alert System
ETN	Evacuee Tracking Network
GIS	Geographic Information Systems
IPAWS	Integrated Public Alert and Warning System
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
RCC	Regional Collaboration Committee
UASI	Urban Area Security Initiative
VTC	Video Teleconferencing
WEA	Wireless Emergency Alerts