Regional Multi-Site Emergency Communication and Training System/ Websites – Scope of Work

Project Overview

The City of Houston Mayor's Office of Homeland Security and Public Safety is seeking a company to design, develop, and deploy three public-facing regional websites—each serving a specific program—with a secure backend. The system should also support inquiry management, dissemination of public information, search engine exclusion to prevent indexing by crawlers, and emergency communication management across three DHS grant-supported focus areas.

The City intends to enter a contract with a qualified firm specializing in website design/ hosting for a term of three (3) years with three (2) one-year options to renew annually, for a maximum five (5) year term.

Project Objectives

- Develop and deploy three branded, accessible, mobile-responsive public websites, each serving program-specific audiences.
- Enable secure login and role-based access for vetted users, ensuring protected access to confidential and grant-related materials.
- Provide user-friendly tools that support communication, inquiry management, and training logistics.
- Ensure interoperability with key enterprise and emergency management systems, including Microsoft 365, Esri ArcGIS Online, and future third-party integrations via documented APIs.
- Implement robust security, compliance, and service-level standards to protect sensitive information and ensure reliable performance.
- Deliver comprehensive support, training, and documentation for system deployment, maintenance, and future scalability.

Summary of Functionality

This platform will enable administrators, volunteers, and stakeholders to collaborate effectively from any location, while ensuring secure, compliant, and reliable service delivery. The solution must provide a secure, cloud-based, software-as-a-service (SaaS) platform with the following core capabilities:

- **Content creation, management, and publishing**, including intuitive, mobile-responsive web content management supporting multiple program sites.
- **Role-based security**, including granular access controls, authenticated sessions, and audit logging to protect sensitive content.

- **Collaboration and inquiry handling**, including tools to support stakeholder communication (e.g., bulk emails, contact groups, surveys/forms with conditional logic) and inquiry management across program audiences.
- **Integration and interoperability**, including compatibility with enterprise systems, such as Microsoft 365 and Esri ArcGIS Online, with documented APIs for future integrations.
- **Scalability and performance**, including infrastructure designed for unlimited users, high availability, and disaster recovery.
- **Accessibility and compliance**, including conformance with Section 508 / WCAG 2.1 AA standards and DHS/FEMA cybersecurity guidance and automated machine translation or manual translation workflows.

Website and Audience Purpose

Regional Coordination of Homeland Security Grant and Programmatic Management Website

- **Audience:** Regional emergency preparedness workgroups, stakeholders, and grant program administrators
- **Features:**
    - Public transparency section, including agendas, meeting outcomes, calendar, news
    - Secure document repository, including grant reports, strategic plans, projects, budgets
    - Secure user logins with role-based permissions
    - Shared access for authorized users from all participating jurisdictions
    - Governance tools for submitting, reviewing, and approving documents

CERT Volunteer Information Website

- **Audience:** Community Emergency Response Team (CERT) volunteers, community members
- **Features:**
    - Volunteer resources, news, alerts, and registration information
    - Interactive training and registration portal, including:
        - The ability to browse upcoming training courses and events
        - Self-service online signup and waitlist management
        - Automated confirmations and reminders via email/SMS
    - Volunteer opportunity signups, including the ability to:
        - View and register for local and regional volunteer events and activations
        - View an opportunity calendar with filters (e.g., location, date, event type)
        - Post event feedback submissions and volunteer hour tracking
    - Volunteer profile management, including the ability to:

        - Access a secure personal profile where volunteers or internal staff can update contact information and availability
        - Track completed training, certifications, and volunteers
        - Download certificates and badges earned
    - A repository of public safety toolkits and instructional documents
    - Inquiry/Contact form
    - Secure login for access to internal documents, sensitive updates, and personalized dashboards
    - The ability to push notifications and newsletters

Technical Capabilities and Support

The software infrastructure must be hosted on a secure, cloud-based virtual private cloud (VPC). Data must be stored in a relational database and accessed via secure web services. To ensure resilience and uninterrupted service, the hosted system must include the following:

- Database clustering and replication.
- Nethreerk load balancing.
- Continuous monitoring of infrastructure health.
- Auto-scaling capacity to handle demand spikes without performance degradation.

The system must support modern security standards, maintain compliance with federal best practices, and provide architecture that is fully auditable and documented.

Platform-Wide Capabilities

The solution must deliver platform-level functionality that enables consistent and secure use across all program websites, including:

- Secure sign-in and role-based access with multifactor authentication (MFA), dashboards, notifications, and audit logging.
- Document and inquiry management with centralized routing, upload/download tracking, and expiration-based file access.
- System setup and migration, including device pre-installation (as needed); default profiles; and transfer of existing files, contacts, and materials.
- Custom programming support to accommodate program-specific workflows (e.g., training tracking, DHS reporting, secure file submission portals, optional e-signature integration).

Integration, Security, and Service-Level Requirements

<u>Integration and Interoperability</u>

The solution must support integration with commonly used emergency management and enterprise platforms. At a minimum:

- Single Sign-On (SSO): The platform must support single sign-on through the City of Houston's enterprise identity provider (Microsoft Azure Active Directory). This capability is a required condition for IT security compliance and must be fully implemented as part of system deployment.
- Collaboration Suites: Support for Microsoft 365 (including Azure AD SSO, calendar, file storage, and Teams integration) or equivalent enterprise platforms.
- Geospatial Systems: Esri ArcGIS Online (AGOL) integration to embed interactive maps, display live data feeds, and provide secure access to geospatial datasets and dashboards.
- API Access: Documented RESTful APIs or equivalent to enable integration with third-party systems (e.g., WebEOC, Everbridge, state/local alerting platforms).
- Extensibility: Vendor must provide a process for requesting, configuring, and testing new integrations throughout the contract.

Usability and Site Administration

The platform must support delegated, non-technical administration:

- Intuitive WYSIWYG editor for no-code content management.
- Mobile-responsive design consistent with regional branding.
    - At a minimum, templates should allow basic customization of navigation, headers, and footers.
    - The vendor is encouraged to describe available template options and any associated costs for additional design services or cafeteria-style variations.
- Compliance with Section 508 / WCAG 2.1 AA standards.
- Role-based admin delegation (assigning edit/publish rights without full admin status).

Secure Content Protection

The platform must protect restricted information from unauthorized access or indexing:

- Authenticated Session Access: Secure files and pages must require login; direct URLs must not bypass controls.
- Search Engine Exclusion: Restricted content must be excluded from indexing by crawlers using server-side controls (robots.txt alone is insufficient).
- Granular Role-Based Permissions: Access control at page, folder, and document levels; example roles include Public, Volunteer, Participant, Admin, Power User, and Reviewer.
- Native File Security: Files must be secured within the platform removing the current necessity to add security to individual files.
- Audit Logging: All secure file access logged (date, user, action). Logs must be exportable for compliance reviews.

Compliance and Best Practices

- Encrypt data in transit (TLS 1.2+) and at rest (AES-256 or equivalent).
- Conform with DHS/FEMA cybersecurity guidance and relevant federal standards, adapted for municipal IT environments.
- Provide documentation of integration architecture, security protocols, and user management procedures.
- All data and content uploaded to or generated within the platform remains the property of the Houston Office of Public Safety and Homeland Security. The vendor must not claim ownership or use such data for any purpose other than providing contracted services.

Service-Level Agreements

- Availability and Performance
  - Minimum 99.9% uptime (monthly), excluding scheduled maintenance (≥72 hours notice).
  - Public pages must load within three seconds under normal conditions.
- Support and Response Times
  - Critical Incidents (system outage, data breach): Acknowledge within 1 hour; resolution or workaround within 4–6 hours.
  - High Priority Issues (major functionality loss): Acknowledge within 2 hours; resolution or workaround within 8–12 hours.
  - Routine Issues (minor bugs, individual user problems): Response within one business day; resolution within five business days.
- Disaster Recovery and Continuity
  - Daily backups stored in geographically redundant facilities.
  - Recovery Point Objective (RPO) ≤ 24 hours; Recovery Time Objective (RTO) ≤ 8 hours for critical services.
  - Vendor must provide a documented disaster recovery plan and conduct at least one annual recovery test, with results shared.
- Reporting and Accountability
  - Vendor must provide monthly uptime/performance reports.
  - SLA credits or penalties apply if availability/response commitments are not met.

Support and Maintenance

The vendor must provide ongoing technical support, maintenance, and updates to ensure the platform remains secure, current, and fully functional. Minimum requirements include:

- Help desk availability with 24/7 coverage for critical issues and defined escalation procedures.
- Regular security patching and feature updates to maintain compliance, functionality, and usability.
- Routine system maintenance including bug fixes, configuration adjustments, and enhancements as needed.
- Administrator and user support through knowledge base resources, documentation, and training refreshers as appropriate.

Deliverables

The vendor must deliver the following project outcomes:

- Three branded public websites, each tailored to its program audience.
- Delivery of branded, mobile-responsive templates for use across program websites. Vendors should also identify optional design services (e.g., cafeteria-style templates or custom layouts) and provide associated pricing as part of their proposal.
- Backend systems that provide secure login and user management, document repository access and tracking, and communication and inquiry management tools.
- Training and documentation, including complete training materials and sessions for administrators and users.
- Deployment and handoff, including system testing, final deployment, and transfer of support documentation.

Optional Services

- The vendor should also identify optional design services (e.g., cafeteria-style templates or custom layouts) and provide associated pricing as part of their proposal.
- The platform should support integration with web analytics tools (e.g., analytics, native dashboards) to monitor usage and engagement. While analytics are not a primary requirement, the vendor should describe available options and indicate any associated setup or licensing costs, so the capability can be activated if needed.

Service Term

Year 1: 10/2026 - 9/2027
Year 2: 10/2027 - 9/2028
Year 3: 10/2028 - 9/2029
Year 4: 10/2029 - 9/2030 option year
Year 5: 10/2030 - 9/2031 option year