

STATEMENT OF WORK

Project Title: Fire and Emergency Medical Services Records Management System (FEMSRMS)

1. Purpose

The Office of the Chief Information Officer (OCIO) on behalf of the Office of Protective Services (OPS) requires a Commercial of the Shelf (COTS) Software as a Service (SaaS) Fire and Emergency Medical Services Records Management System to replace outdated, manual and fragmented systems. The vendor shall provide a secure system that is aligned with industry standards to support OPS's strategic commitment to safeguard NASA personnel, infrastructures and mission-critical operations.

2. Goals and Objectives

NASA seeks a COTS FEMSRMS system along with professional services for the configuration, implementation and integration of 7 operational stations and one independent non-production test environment. The FEMSRMS system shall be a Federal Risk and Authorization Management Program (FedRAMP) High Authorized cloud-based configured COTS offering at the time of award.

The NASA Office of Protective Services and Office of the Chief Information Officer have established the following objectives:

- Replace the existing manual and fragmented Fire and EMS Records Management Systems with a FedRAMP High Authorized cloud-based solution that meets Federal Regulations and NASA OPS and OCIO requirements.
- Achieve Agency Authority to Operate (ATO), in accordance with NASA Procedural Requirement (NPR) 7120.7, prior to the go live date for the FEMSRMS.
- Enable site consolidation allowing data sharing.
- Enhanced reporting and analytics capability.
- Achieve cost savings through efficiencies gained from reducing the number of solutions maintained/supported.
- Have a fully operational system that can integrate with Central Square CAD and ESRI/ArcGIS.

3. Scope

3.1 Software Functional Standards

3.1.1 Incident Reporting & Fire Documentation:

- Ability to create fire/incident reports and emergency response documentation with Fire Risk Management Service (FRMS) capture.
- National Emergency Response Information System (NERIS) v1 connectivity and a National Fire Incident Reporting System (NFRIS) legacy crosswalk for reporting.
- Fire reporting must also include analytics.

3.1.2 Electronic Patient Care Report (ePCR) & Hospital Data Exchange:

- National Emergency Medical Services Information System (NEMSIS) compliant electronic patient care reporting that is Health Insurance Portability and Accountability Act (HIPAA) compliant, to include a HIPAA compliant hospital handoff packet.
- Allow for cardiac monitor integration that enables real-time sharing of pre-hospital patient care reports, EKGs, and vital signs between Emergency Medical Services (EMS) and receiving hospital cardiac care units.
- Supports HIPAA compliant encrypted one-way digital transfers to receiving facilities.

3.1.3 CAD Ingestion & Mobile Responder/Notifications:

- Vendor-agnostic Central Square CAD interface.
- Mobile responder capability (notifications and incident access on any device).
- Offline-capable mobile cache with sync-on-reconnect for intermittent-connectivity sites (e.g., White Sands, Stennis)

3.1.4 Pre-Incident Planning:

- Ability to build pre-incident plans for response personnel. Pre-incident plans shall include field-ready documentation detailing property or building's specific layout/floor plan, associated hazards, available water sources to include pre-identified hose-lay calculations, exterior exposures, and immediate assets.
- Include mapping, plan management, response, and occupancy hazards

3.1.5 Fire Prevention:

- Including inspections, permits, and occupancies

3.1.6 Connections to ESRI/ArcGIS for mapping, hydrant and water supply tracking.

3.1.7 Hydrants module:

- Module must include service and testing, water source tracking and availability with a hose lay calculator.

3.1.8 Facility Inspections, pre-plans, and Inspect-Test-Maintain (ITM)

- Provide Mobile inspection and pre-plan workflows with deficiency tracking
- ITM management
- Ability to create reports that include trends on inspection compliance.

3.1.9 Personnel Scheduling & Rostering:

- Provide for a centralized personnel records repository
- Provide Roster and Leave Management
- Ability to track personnel qualifications.
- Auto shift-coverage proposals. System will automatically identify available personnel to fill a vacant shift, with Shift Officer final approval.
- Provide automated staffing notifications.

3.1.10 Training, Virtual Training & Compliance:

- Integrated online training with a course catalog.
 - Ability to connect to NASA Fire Services Training Academy and integrate with NASA ProBoard.
- Provide the ability to track completion records.
- Ability to track Continuing Education Units (CEU) credit offerings. System needs to be able to provide locations where employees can take courses required to maintain certifications.
- Allow for trainings courses to be assigned based on shift, crew or individual.
 - System should notify users of available training for the month.
 - System should allow users to select the training they wish to attend.
 - System should allow the training officer to input back-up dates for training.
- Certification-expiry alerts delivered via email to notify Users and their associated Supervisors of assigned trainings that are due. Alerts should be sent at the following intervals; 90-days, 60-days, and 30-days. At the 30-day interval and when training is overdue system shall escalate alerts to the associated Fire Chief.
- Provide the ability to create training plans.

- Allows for the tracking for events and activities to include a daily log that captures all training activities completed.
- Allow for credential and compliance management.

3.1.11 Exposure Tracking & Health/Wellness

- System shall provide per-responder, per-incident exposure history.
- Cancer-presumption alignment in accordance with National Fire Protection Association (NFPA) 1500.
 - System shall provide users with a questionnaire based on the incident responded to.
 - System shall notify users of the next steps based on responses to the questionnaire.
 - System shall notify the individual and supervisor regardless of a possible exposure occurred or not.
- System should provide health/wellness documentation and reporting.
- Exposure tracking & health/wellness must be able to connect to incidents.

3.1.12 Incident Command & On-Scene-Accountability:

- System must provide embedded access to Incident Command System (ICS) form sets. Forms should be available based on specific incidents responded to. All required forms can be found on FEMA ICS Resource Center webpage ([ICS Resource Center](#)).
- System shall provide Tactical worksheets.
- Allow for resource and action-item tracking.
- Provide personnel accountability at an incident, allowing supervisors to track the location, assignment, and safety of every responder operating in a hazardous zone.
- System should provide an Incident board to include incident trackers and incident timers.
- System should provide after-action reviews.

3.1.13 Assets and Inventory:

- Provide fleet equipment and inventory management.
- Asset register for apparatus and equipment.
- Allow maintenance scheduling to include Out of Service (OOS) tracking for vehicles, tools and equipment.
- Allow recall management

- Provide inspections and lifecycle/supply tracking.
- Provide medication tracking.
- Allow daily and monthly asset check-outs.

3.1.14 Narcotics & Controlled-Substance Management:

- Drug Enforcement Agency (DEA)-compliant chain-of-custody for tracking narcotics.
- System must be able to track witnessed waste, reconciliation, and controlled substance tracking integrated with asset/inventory controls.

3.1.15 Investigations & Evidence Management:

- Provide fire cause-and-origin documentation with center configured customizable investigation forms.
- Provide full evidence chain-of-custody tracking, with the ability to include scene details.

3.1.16 Events, Activities & Non-Incident Records:

- Ability to capture and report daily departmental activities and non-incident events.

3.1.17 Data, Analytics & Reporting:

- System shall provide incident analytics, compliance and inspection-trend reports, and exportable data for downstream use.
 - Data needs to be exportable in the following formats: CSV, Excel, Word, and PDF.

3.2 Accessibility:

- Section 508 compliance. NASA is committed to providing accessible Information and Communication Technology (ICT) to individuals with disabilities, including members of the public and federal employees. The contractor-provided solution shall meet or exceed all requirements of section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).

3.3 Security Requirements:

- The contractor-provided solution shall support a secure, multi-factor authentication (MFA) method for Government-consuming end users to access the service and for Government personnel who will perform

administrative duties. The contractor shall support the integration of a multi-factor NASA authentication services to include Single Sign-On (SSO) and Federal Government Personal Identity Verification (PIV) Card access. A user inside NASA's firewall shall be able to access the system without having to provide separate credentials. The system shall support an MFA solution that aligns with all applicable Federal IT security standards and policies. These policies include session timeouts and inactive user lockouts. The information system/IT solution shall support role-based access controls to distinguish between end users need access to different levels of data (e.g. end users only needing access to non-sensitive data and end users needing access to sensitive data). At a minimum assignable end-user roles shall include the following: Administrators, Supervisors, Instructors and firefighters.

3.4 FedRAMP High Authorization:

- The Contractor shall have and maintain an active FedRAMP High Authorization for the proposed Software as a Service (SaaS) solution. FedRAMP High Authorization shall cover the complete SaaS boundary to include web applications, APIs, microservices, and integrated add-ons throughout the entire period of performance.
 - If the SaaS solution relies on underlying Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) providers (e.g., AWS GovCloud, Microsoft Azure Government), the Contractor shall ensure that all underlying services maintain an active FedRAMP High Authorization. Any change to the hosting provider, datacenter region, or boundary inheritance requires formal pre-authorization granted by the Agency Authorizing Official (AO).
 - The Contractor shall not introduce new commercial third-party integrations, external microservices, or subprocessors into the FedRAMP High boundary without a formal Significant Change Request (SCR) approved by the FedRAMP Program Management Office (PMO) and the Agency AO.
- In the event of a lapse, suspension or revocation of the SaaS product's FedRAMP High Authorization:
 - Immediate Subscription Suspension and Prorated Credits:
 - The Government shall not be obligated to pay recurring subscription, license, or user maintenance fees for any period

during which the SaaS application is out of FedRAMP High compliance.

- The contractor shall provide a direct prorated credit or refund for all prepaid SaaS subscription fees corresponding to the non-compliant duration.
- Unrestricted SaaS Data Egress and API Access:
 - The Contractor shall immediately lift any standard rate limits, bandwidth restrictions, or egress fees to allow rapid, programmatic extraction of all Government data.
 - Data must be exportable via bulk automated REST APIs or secure download in open, machine-readable formats (e.g., standard JSON, CSV, flat files, and raw relational database schemas with metadata).
 - The Contractor shall deliver a complete data dictionary and entity relationship diagrams (ERDs) within forty-eight (48) hours of the lapse to ensure seamless data reconstruction.
- Data Transition and Continuity Support:
 - The Contractor shall maintain a read-only, hardened instance of the SaaS tenant environment for up to one hundred eighty (180) calendar days to facilitate transition to an alternate FedRAMP High-authorized SaaS provider at no additional cost to the Government.
- Contract Termination for Cause:
 - Failure to restore FedRAMP High status within thirty (30) calendar days after a lapse, suspension or revocation will result in a termination for cause in accordance with FAR 52.212-4(m).
- Logical Sanitization and Cryptographic Erasure:
 - Upon receipt of written verification by the Government that all tenant data has been successfully extracted, the Contractor shall execute logical sanitization and cryptographic key destruction in accordance with NIST SP 800-88 Rev. 1 across all multi-tenant databases, logs, backups, and caching layers.
 - A signed Certificate of Sanitization shall be delivered to the CO within fifteen (15) calendar days after receiving Government confirmation of successful data extraction.

3.5 Professional Services and License Management:

- The contractor shall provide all material, equipment, and labor to perform all tasks associated with licensing, hosting, configuration, testing, integration, implementation, training, and administration of the contractor provided FEMSRMS solution. This shall include, but is not limited to, technical implementation of all system enhancements including beta testing, minor releases, major releases, software updates, and configuration changes.
 - The solution will provide 7 operational stations as follows:
 - 2 stations at Kennedy Space Center (KSC)
 - 1 CAD connection license
 - 2 stations at Wallops Flight Facility (WFF)
 - 1 station at Stennis Space Center (SSC)
 - 1 station at Ames Research Center (ARC)
 - 1 station at White Sands Test Facility (WSTF)
 - Program service licenses to include HIPAA certification and authentication enablement licenses for all operational stations.
 - The solution will provide for one separate non-production test/sandbox environment for training and configuration testing.
- The contractor shall furnish all management, supervision, labor, equipment, and materials unless otherwise specified.
- Coordinate with Government Personnel and assist with achieving Authority to Operate (ATO).
- Maintain project schedules, tentative project schedule is as follows:

Milestone	Schedule / Due Date
Project Kickoff Meeting	NLT 15 days after contract award
System Configuration Completion	February 2027
Receive IT Security ATO	NLT April 2027
Training for KSC	May 2027
Go Live for KSC Operational Stations	May 2027
Training for Remaining Centers (WFF, SSC, ARC, WSTF)	May 2027
Remaining Center Go Live	May 2027

4. Place of Performance

All work associated with the performance of this contract shall be performed off-site. Access to NASA Centers, Sites, and Facilities will not be required.

5. Period of Performance

The base year shall include all activities up to the receipt of ATO for the FEMSRMS solution.

Base Period: October 2026 – May 2027

Option Years:

Option Year One shall include the following:

- Licensing for 7 operational stations, non-production test environment, CAD connections, and program services as listed in Section 3.5.
- Virtual User Training for each operational license tailored to specific user roles, to cover all relevant functionalities. All training sessions are expected to be recorded and saved for offline viewing.

Option Year 2 through 3 shall only include the recurring subscriptions for all licenses as listed in Section 3.5.

Option Year 1: May 2027 – May 2028

Option Year 2: May 2028 – May 2029

Option Year 3: May 2029 – May 2030