SOURCES SOUGHT / REQUEST FOR INFORMATION (RFI)

FOR

ELECTRONIC SECURITY SYSTEM (ESS) FOR NAVAL HOSPITAL BREMERTON

Reference Number: HT941026N0067
Issued Date: 09June 2026
Questions Due: 18 June 2026
Response Due Date: 24 June 2026, 11:00 AM Pacific Time

Issued By: Defense Health Agency Contracting Activity (DHACA) in San Diego, CA

NAICS Code: 561621 – Security Systems Services (except Locksmiths)
Product Service Code: N063 – Installation of Equipment/Security and Alarm Systems

DISCLAIMER:

This Sources Sought/RFI is issued solely for information and planning purposes. It does not constitute a solicitation or a promise to issue a solicitation in the future. This notice does not commit the U.S. Government to contract for any supply or service. Further, the Government is not currently seeking proposals and will not accept unsolicited proposals. Respondents are advised that the U.S. Government will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future solicitation, if any is issued.

1.0 DESCRIPTION & BACKGROUND

The Defense Health Agency (DHA) is seeking information on sources capable of providing a comprehensive, integrated, and cyber-secure Electronic Security System (ESS) for Naval Hospital Bremerton (NHB). The Government's objective is to procure, install, and/or modernize its ESS to be compliant with applicable governance to protect personnel, patients, assets, and sensitive information.

The required solution involves the design, procurement, installation, testing, and accreditation of a complete and fully operational ESS. The system must integrate several subsystems, including, but not limited to, an Intrusion Detection System (IDS), an Access Control System (ACS), and a Video Surveillance System (VSS). These subsystems must be managed under a single, unified Physical Security Information Management (PSIM) or similar central management platform.

The system must be compliant with all relevant Department of Defense (DoD), Unified Facilities Criteria (UFC), and DHA directives, including stringent cybersecurity requirements under the

DoD Risk Management Framework (RMF) to achieve and maintain an Authority to Operate (ATO). The unique environment of a military medical facility requires full compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

2.0 PURPOSE

The purpose of this Sources Sought/RFI is to conduct market research, which will assist the Government in developing its procurement strategy. The Government is seeking to identify qualified and experienced sources, particularly small businesses, capable of meeting the requirements. The information received will help determine the availability of commercial solutions, potential procurement approaches, and the appropriate contracting vehicle.

3.0 REQUESTED INFORMATION & CAPABILITY STATEMENT REQUIREMENTS

Respondents are requested to submit a capability statement that addresses the following areas. Please limit your response to no more than ten (10) pages.

3.1 Company Information:

- Company Name, Address, and Website.
- Unique Entity Identifier (UEI), CAGE Code, and business size/socio-economic status under NAICS code 561621 (e.g., Small Business, 8(a), Service-Disabled Veteran-Owned Small Business (SDVOSB), HUBZone, Woman-Owned Small Business (WOSB), etc.).
- Point of Contact (Name, Title, Phone Number, and E-mail Address).
- Any relevant Government-wide Acquisition Contracts (GWACs) or GSA Schedule contracts held.

3.2 Relevant Experience:

Please provide at least two (2) and no more than four (4) examples of projects of similar size, scope, and complexity performed within the last five (5) years. For each project, please provide:

- Contract number, total dollar value, and period of performance.
- Client name (specifically note if the client was DoD, DHA, or another federal agency).
- A brief description of the work performed, highlighting its relevance to this requirement. Specifically address your experience with:
    - Installing and integrating multi-vendor ACS, IDS, and VSS subsystems in a hospital or similar sensitive environment.
    - Implementing a PSIM or similar central management platform.
    - Adhering to UFC 4-021-02, UFC 4-010-06, and other relevant DoD standards.

- Navigating the full DoD Risk Management Framework (RMF) lifecycle for a Platform IT (PIT) or Facility-Related Control System (FRCS) to achieve an ATO.
- Ensuring system and procedural compliance with HIPAA in a healthcare setting.

3.3 Technical Approach & Capabilities:

- Briefly describe your company's technical approach to designing, installing, and accrediting a compliant ESS in a 24/7 operational hospital environment, minimizing disruption to patient care.
- Describe your capabilities and corporate experience in managing complex cybersecurity accreditation processes under RMF.
- Describe your company's quality control processes for ensuring system reliability and adherence to performance standards (e.g., availability, false alarm rates).
- Based on a review of the draft PWS, identify which of the following Courses of Action (COAs) is recommended to the Government and describe why:
    - COA #1: System Repair and Restoration: Fix the current, existing ESS, including all inoperable cameras, and ensure it meets baseline operational requirements.
    - COA #2: Full System Replacement and Upgrade: Replace and upgrade the entire VSS. Install new cameras in all locations required by UFC 4-510-01, Section 5-4.8.1.
    - COA #3: System and Camera Replacement: Replace and upgrade the current VSS, replace all currently installed cameras, and install new cameras in required locations as needed to meet UFC requirements.
    - COA #4: Full System Replacement with IDS/ACS: Same as Option 2, but also includes the complete replacement and upgrade of the IDS and ACS systems.
    - COA #5: Comprehensive System and Component Replacement: Same as Option 3, but also includes the complete replacement and upgrade of the IDS and ACS systems.
- Describe the following maintenance-related content:
    - Terms, duration, and coverage of the standard warranty for all furnished supplies and services.
    - Preventative maintenance: Outline the frequency and scope of preventative maintenance visits (e.g., cleaning, testing, and calibration) to ensure optimal system performance
    - Emergency repairs: Describe a tiered response plan for critical and routine failures, defining the on-site response commitment for each.
    - Cybersecurity Maintenance: Describe your strategy for providing quarterly offline updates (e.g., patches, antivirus, and firmware) to maintain the system's Risk Management Framework (RMF) authorization post-acceptance.

3.4 Market Research Pricing:

Provide a market research pricing for your recommended COA in Attachment 2 – COA Market Research Price to include pricing for any products/supplies/equipment, emergency repairs and preventative maintenance.

3.5 Teaming and Subcontracting:

- Describe your anticipated teaming arrangements or subcontracting strategy for a project of this nature.
- Identify key functional areas you would typically perform in-house versus those you would subcontract (e.g., cybersecurity accreditation, electrical work, specific system programming).

4.0 SUBMISSION INSTRUCTIONS

Any interested party that believes they are capable of meeting the requirement as described herein may identify their interest and capabilities in response to this request for information. Responses must be submitted in writing via email no later than 11:00 AM PDT on 24 June 2026. Email submissions should include the Notice of Intent Reference number: HT941026N0067 in the subject line of the email. Telephone responses and requests will not be accepted. A determination by the Government not to compete the requirement based on responses to this notice is solely within the discretion of the Government.

Interested parties are requested to submit their capability statements electronically via email to the points of contact listed below.

- Primary Point of Contact:
    - Nickolas Romero, Contract Specialist, nickolas.e.romero.civ@health.mil
- Secondary Point of Contact:
    - Jasmin Rooker, Contracting Officer, jasmin.m.rooker.civ@health.mil

All responding vendors must be registered to the System for Award Management (SAM). Information can be found at https://www.sam.gov. Complete SAM registration means a registered Unique Entity ID (UEI) and CAGE.

The email subject line must read: "Response to Sources Sought/RFI **HT941026N0067** – [Your Company's Name]".

Responses shall be submitted in PDF (adobe Acrobat) format. Do not submit marketing materials as these will not be reviewed.

Questions regarding this Notice shall be submitted in writing via e-mail to the points of contact listed above. No telephone inquiries will be accepted. The Government does not guarantee all questions will be answered.