REQUEST FOR INFORMATION (RFI) #842571563

AMMENDMENT 01: This amendment extends the response date until March 28, 2025, at 2:00 pm EST

The Defense Information Systems Agency Program Executive Office (DISA PEO) / Program Baseline Support, SD12 / Defense Information Contracting Organization PS8414 is seeking information from industry to assist with the development and planning of a potential new requirement.

THIS IS A REQUEST FOR INFORMATION (RFI) NOTICE ONLY. THIS IS NOT A REQUEST FOR PROPOSALS (RFP). NO SOLICITATION IS AVAILABLE AT THIS TIME.

1. **Overview/Purpose/ Description of Procurement**
   The DISA PEO is seeking to capture information on industry capabilities to develop and deploy the Department of Defense (DoD) Emergency Services Internet Protocol Network (D-ESInet). DISA is looking to gather Rough Order of Magnitude (ROM) information for such an effort along with information on innovative strategies and feedback for development and deployment of D-ESInet. **DISA is looking to deploy the service in two phases a. Initial Operational Capability to encompass CONUS and b. Full Operational Capability to encompass OCONUS. Therefore, the cost estimates will reflect two distinct phases. Please note, the Government will not pay for information received in response to the RFI.** The Government will consider feasible technical approaches, including the use of Commercial-off-the-Shelf (COTS) technology and open standards.

2. **Scope of Effort**
   DISA is seeking information on the design, implementation, test, operation, and sustainment of a D-ESInet system that meets the operational needs of DoD emergency services community. The D-ESInet must be designed to provide a secure, reliable, and interoperable network infrastructure to deliver emergency calls to the right DoD Public Safety Answering Points (PSAPs) for emergency services.

   DISA is also seeking a capability statement. Interested businesses shall submit a brief capabilities statement (no more than three pages) demonstrating the ability to perform the services, as described in the sections below.

3. **Technical Characteristics**

   The D-ESInet service is responsible for managing and facilitating the routing of emergency calls to the appropriate DoD or commercial PSAP that can manage the incident. Specifically, D-ESInet does *not* include:

- Initial Call Setup and Routing – The connectivity and services necessary to route a call from the individual experiencing an incident to the ESInet are part of the broader DoD infrastructure, but outside the scope of D-ESInet. Examples of these external systems include both physical telephony networks such as DISA Enterprise VoIP (EVoIP) and cloud-based collaboration systems such as DoD365 Teams.

- Dispatching from PSAPs – Once the D-ESInet delivers a call to the appropriate PSAP, any further connectivity to first responders will be managed through Computer Aided Dispatch (CAD) systems that are also outside the scope of the DoD ESInet.

The D-ESInet system will be developed and deployed in two increments. The key requirements for each increment are as follows:

- Increment 1: Initial Operating Capability (IOC) increment for basic service functionality, including network infrastructure in the Continental United States (CONUS), data management, and administrator interface.

- Increment 2: Build on the first increment to provide CONUS and Outside the Continental United States (OCONUS) Full Operational Capability (FOC), including all planned features and functionality.

Each increment will be developed and deployed with continuous testing and evaluation to ensure that the D-ESInet meets the required standards.

To Industry: Proposed solutions will take into consideration security, scalability, performance monitoring, and a disaster recovery plan. Is your proposed solution extensible such that it will support a global D-ESInet?

Notional Architecture

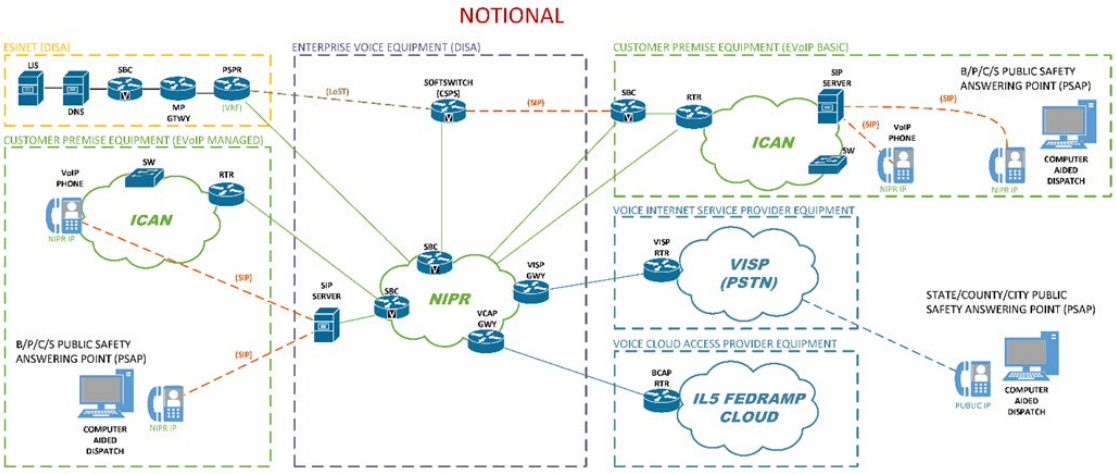

Figure 1: D-ESInet Notional Architecture (Source – DISA)

As depicted in Figure 1, D-ESInet is a unique service offering that facilitates collaboration amongst multiple stakeholders, including emergency service agencies, industry partners, and Government agencies. Specifically, users of the service would include Emergency Management Agencies (local, state and federal emergency management agencies), first responders (police, fire and medical responders), and DoD organizations (military units and Defense agencies).

The intent of the service is to deliver 911/ Next Generation (NG) 911 calls to the appropriate DoD PSAP. D-ESInet will be integrated with other systems and services, including Public Safety Answering Points (PSAPs), commercial ESInet, emergency management systems, incident management systems, and communication systems.

Key Architecture Characteristics

- Open Architecture: The ESInet service will be designed with an open architecture to ensure interoperability with other emergency services and DoD systems.
- Common Data Standards: The service will use common data standards to ensure seamless data sharing.
- Service-Oriented Architecture (SOA): The service will be designed using an SOA approach to ensure flexibility and scalability.
- Cloud-Based: The service will be DoDIN hosted cloud-based to ensure resilience/reliability scalability, flexibility, and cost-effectiveness, and will comply with Department of Defense Cloud Computing Security Requirements Guide (SCCA) version 1, release 3 DOD, 2017.
- IPv6 Capability: All products will support both Internet Protocol v4(IPv4) and v6 (IPv6) stacks as described in RFC 8200. IPv6 will also be implemented IAW with USGv6 Capability Summary Strings (CSS) for all network devices found in this system.

To Industry: Provide an assessment regarding Figure 1: D-ESInet Notional Architecture (Source – DISA)

To Industry: Describe your approach to ensuring consistent performance, minimizing downtime (reliability) and ability to continue operating in the face of adverse conditions, attacks or other disruptions(survivability)

To Industry: Describe your implementation of a disaster recovery test plan.

System Overview

The D-ESInet will consist of the following major subsystems:

- Network Infrastructure: A high-availability, scalable, virtual IP network infrastructure that supports secure data transmission and communication. This includes, but is not limited to:
    - Redundant and diverse network connections to ensure maximum uptime and availability.
    - Implement a Quality of Service (QoS)-type of capability to prioritize ESInet traffic in a congested environment. Compliance with USGv6 and IPv6 mandates.
    - Compliance with relevant industry standards, such as NENA i3 and NG9-1-1.

- Data Management: A comprehensive data management system that captures, stores, and manages emergency services data, including:
    - Processing and parsing of Presence Information Data Format – Location Object (PIDF-LO) metadata to extract relevant information for emergency response.
    - Supports the DISA Softswitch architecture to enable seamless emergency communication and call routing.
    - Supports legacy TDM and PBX systems to enable seamless emergency communication and call routing if a mission partner gateway (MPG) to the legacy ESInet is implemented.
    - Support for data analytics and reporting to facilitate informed decision-making and system optimization.

- User Interface: D-ESInet will have a user-friendly interface that provides intuitive access to system functionality and features, including configurable dashboards and workflows to support emergency response operations.

System Technical Requirements

The key technical requirements of the D-ESInet service are summarized in the sub-sections below**.**

Architecture Characteristics

- The system will provide emergency service for calls which may originate from many kinds of devices and services, to include multimedia (i.e., audio, video, text).

- The service will provide for emergency calls that are destined to be answered at the i3 PSAP and may originate as either legacy or IP-based calls.
- The service will provide for all calls signaled with SIP audio, video, interactive text, and/or instant messaging media.
- The service will provide a signaling protocol primarily based on SIP Connect 2.0.

- All inter D-ESInet calls will use Transport Layer Security (TLS).

Basic Services Data Characteristics

- The service will provide data associated with the call in an XML data structure retrieved from a web service, to be operated by the origin network or a contractor.
- The service will provide a location in an XML data structure retrieved from a web service.
- The service will provide data associated with a caller in an XML data structure retrieved from a web service, which shall include a header containing the URI for the data associated with the caller.
- The service will provide the ability for call and data Logging. Every Call for Service (CFS) event occurring on the ESInet SHALL be logged on the service. Log Events include: any incident related media; data and time stamp; agency; agent (if appropriate); call and Incident IDs (if appropriate); and an Event Type.

Security Characteristics

- The service will provide authentication by implementing strong authentication for their administrators by employing two or three factor smartcards, passwords, and/or biometrics.
- The service will use Security Assertion Markup Language (SAML) for interagency communications. To the extent possible, all services and facilities in the D-ESInet shall provide "Single Sign On" using SAML.
- The service will provide a source of credentials for authentication. The PSAP Public Key Infrastructure (PKI) shall provide a public key certificate to each PSAP and to service providers providing services on one or more ESInet(s).
- The service will meet applicable Cybersecurity (CS) Risk Management Framework requirements and receive an Authority to Operate (ATO)/Authority to Connect (ATC).
- The system will be configured to be audited, or otherwise verified, on a regular basis.

System Interfaces

- The service will provide integration / interfaces with other systems (i.e., DoD Softswitches, SBCs, Session Controllers, and VISP infrastructure) as well as commercial ESInets.
- The service will operate IAW the National Emergency Number Association (NENA) i3 Standard for Next Generation 9-1-1 (NG911) GIS Data Model [11].

IPv4/IPv6

- The service will support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) stacks as described in RFC 8200. IPv6 will also be implemented IAW USGv6 Capability Summary Strings (CSS) for each device type listed.

  To Industry: Does the requirement for a DoD hosted D-ESInet limit the capabilities proposed by your solution. If so, what are those limits? What additional capabilities would be offered by hosting the solution in an Impact Level 5 (IL-5) commercial cloud?

  To Industry: Describe how your proposed solution satisfies the applicable DoD Security Technical Implementation Guides (STIGs) and Security Requirements Guide (SRG) to include FIPS 140 requirement.

4. **Requested Information**
   The Government currently does not have any existing Government-Wide Acquisition Contracts that align with the scope of the requirements outlined in this request. The information provided will help the Government determine the most suitable procurement method or approach.

   Responses may include pricing information, such as a Rough Order of Magnitude (ROM), but will not be as detailed as a formal price proposal. Additionally, please provide any suggestions or recommendations you may have for the Government's consideration regarding this request.

   To assist DISA in determining the level of participation by small business in any subsequent procurement that may result from this RFI, provide information regarding any plans to use joint ventures (JVs) or partnering. Please outline the company's areas of expertise and those of any proposed JV/partner who combined can meet the specific requirements contained in this notice.

RESPONSE GUIDELINES:

Interested parties are requested to respond to this RFI with a white paper. Submissions cannot exceed 20, single spaced, 12-point type with at least one-inch margins on 8 1/2" X 11" page size. The response will not exceed a 5 MB e-mail limit for all items associated with the RFI response. Responses must specifically describe the contractor's capability to meet the requirements outlined in this RFI. Oral communications are not permissible. SAM.gov will be the sole repository for all information related to this RFI.

Companies who wish to respond to this RFI will send responses via email no later than 2:00 p.m. Eastern on **March 28, 2025**, to tricia.l.singler.civ@mail and kari.r.wuebbles.civ@mail.mil.

INDUSTRY DISCUSSIONS:

DISA representatives may choose to meet with potential offerors and hold one-on-one discussions. Such discussions would only be intended to obtain further clarification of potential capability to meet the requirements, including any development and certification risks.

QUESTIONS:

Questions regarding this announcement shall be submitted in writing by e-mail to tricia.l.singler.civ@mail.mil and kari.r.wuebbles.civ@mail.mil. Verbal questions will NOT be accepted. Answers to questions will be posted to SAM.gov. The Government does not guarantee that questions received after 2:00 p.m. Eastern on **March 28, 2025**, will be answered. The Government will not reimburse companies for any costs associated with the submissions of their responses

RECAP OF QUESTIONS TO INDUSTRY:

- Provide an assessment regarding Figure 1: D-ESInet Notional Architecture (Source – DISA)
- Does the requirement for a DoD hosted D-ESInet limit the capabilities proposed by your solution. If so, what are those limits? What additional capabilities would be offered by hosting the solution in an Impact Level 5 (IL-5) commercial cloud?
- Describe how your proposed solution satisfies the applicable DoD Security Technical Implementation Guides (STIGs) and Security Requirements Guide (SRG) to include FIPS 140 requirement.
- Proposed solutions will take into consideration security, scalability, performance monitoring, and a disaster recovery plan. Is your proposed solution extensible such that it will support a global D-ESInet?
- Describe your approach to ensuring consistent performance, minimizing downtime (reliability) and ability to continue operating in the face of adverse conditions, attacks or other disruptions(survivability)
- Describe your implementation of a disaster recovery test plan.
- Provide ROM for your solution for D-ESInet CONUS & ROM for D-ESInet OCONUS
- Provide a Capability Statement.

DISCLAIMER:

This RFI is not a Request for Proposal (RFP) and is not to be construed as a commitment by the Government to issue a solicitation or ultimately award a contract. Responses will not be considered as proposals nor will any award be made as a result of this synopsis.

All information contained in the RFI is preliminary as well as subject to modification and is in no way binding on the Government. FAR clause 52.215-3, “Request for Information or Solicitation for Planning Purposes”, is incorporated by reference in this RFI. The Government does not intend to pay for information received in response to this RFI. Responders to this invitation are solely responsible for all expenses associated with responding to this RFI. This RFI will be the basis for collecting information on capabilities available. This RFI is issued solely for information and planning purposes. Proprietary information and trade secrets, if any,

must be clearly marked on all materials. All information received in this RFI that is marked "Proprietary" will be handled accordingly. Please be advised that all submissions become Government property and will not be returned nor will receipt be confirmed. In accordance with FAR 15.201(e), responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract.