Contract Opportunity

Version Current Record

- Pre-Award
- Solicitation Details
- Classification
- Description
- Contact Information
- Attachments/L

NAS Cyber Information Security and Operations

Opportunity
Active

Notice ID
693KA8-26-R-00009

Related Notice
(blank)

Contract Opportunity Type
Sources Sought

Contract Line Item Number
(blank)

Inactive Dates
Apr 02, 2026

Inactive Policy
15 days after re-sponse date

Response Date
Mar 18, 2026 6:00 PM EDT

Published Date
Mar 11, 2026 1:34 PM EDT

Department/Ind. Agency
TRANSPORTA-TION, DEPART-MENT OF

Sub-tier
FEDERAL AVIA-TION ADMINISTRA-TION

Office
693JF9 HEAD-QUAR-TERS

Classification

Original Set Aside
Total Small Business Set-Aside (FAR 19.5)

Product Service Code
DB02 - IT AND TELECOM - COMPUTE SUPPORT SERVICES, NON-HPC (LABOR)

NAICS Code
541519 - Other Computer Related Services

Place of Performance
(blank)

Initiative
None

Description

1. INTRODUCTION

Cybersecurity is a critical component of national security and economic stability with the increasing integration of networked systems, connected devices, and digital platforms across the aviation ecosystem. Cyberspace is a vital domain for the Federal Aviation Administration (FAA). The FAA relies on secure, resilient information systems in cyberspace to fulfill its mission to ensure safe and efficient air travel.

The growing sophistication of cyber threats ranging from nation-state actors to independent malicious groups adver-

saries poses a significant threat to the FAA's cyberspace infrastructure. They actively target government networks, and some have demonstrated the capability to disrupt and/or compromise elements of the FAA's information environment. As these threats from adversaries evolve, the FAA must strengthen its cybersecurity posture to protect its systems, maintain operational continuity, and safeguard the integrity of the National Airspace System (NAS).

The purpose of this market survey is to (1) gather information about potential vendors and their capabilities and (2) obtain vendors' comments and recommendations regarding draft requirements in accordance with the FAA Acquisition Management System (AMS) Policy 3.2.1.2.1. This announcement is not a Screening Information Request (SIR) or Request for Proposals (RFP). The FAA is not seeking or accepting unsolicited proposals. The FAA will not pay for any information received or cost incurred in preparing the responses to this market survey or associated activities. Therefore, any costs associated with the submission of responses are solely at the interested vendor's expense.

The nature of the competition that will be conducted for this procurement has not been finalized at this time. The FAA will review the responses to this market survey and will make acquisition decisions based on vendor responses and the FAA's needs.

This market survey must not be construed as an obligation on the part of

the FAA to acquire these services. Since this is not an SIR or RFP, no results will be issued to the responding firms. No solicitation for these items exists at this time. If a solicitation is issued, it will be announced on the SAM.gov website. It is the vendor's responsibility to monitor the website for release of the solicitation.

The FAA may request that one, some, all, or none of the responders to the market survey provide additional information. No evaluation of vendors will occur based on this additional information, and vendor participation in any informational session is not a promise of future business with the FAA. The FAA reserves the right to have communication with any or none of the respondents. A response to this market survey is not a prerequisite for future procurement consideration.

All information provided in response to this market survey except that which qualifies under an exemption may be subject to release under the Freedom of Information Act (FOIA). Information considered proprietary or confidential must be clearly marked as such and the vendor must provide justification to the FAA of such designation if requested. Any information not identified as proprietary or confidential will be used at the FAA's discretion and may be publicly released without further FOIA disclosure review by the FAA or respondent(s).

Any amendment(s) issued to this announcement will be published on SAM.gov. It is the interested parties' respon-

sibility to visit this website frequently to be informed of any changes to this announcement. Note: the FAR references cited in SAM.gov are not applicable to this market survey as the FAA has its own acquisition policies and guidance contained in AMS.

2. BACKGROUND

The Air Traffic Organization (ATO) has a critical infrastructure and the Cyber Security Strategic Plan advances progress towards a National Airspace System (NAS) where it remains secure and resilient. The plan also provides support for critical and essential services to continue and function under a range of cyber conditions. The NAS cybersecurity capabilities must adapt to changing cyber threats. This includes NAS operations that can withstand and/or rapidly recover from disruptions.

The sustainment of NAS Cyber Operations (NCO), Independent Risk Assessment capabilities, and Information Systems Security (ISS) Assurance is critical to fulfilling the requirements of the Office of Management and Budget's (OMB) for continuous monitoring requirement, as well as complying with Federal Information Security Management Act (FISMA), and Executive Order 13636, Presidential Policy Directive (PPD-21) and the ATO Cyber Security Strategic Plan.

Within the FAA there are three distinct cyber domains: NAS (operational/critical infrastructure), Research and Development, and Mission Support (IT). This Statement of Work (SOW) presents support requirements necessary for the

NAS systems that reside both in the NAS Operational domain as well as the Mission Support (MS) domain.

3. DESCRIPTION/SCOPE

The FAA anticipates requirements to support cybersecurity testing, risk assessment and operational security services within the National Airspace System (NAS). These services involve complex operational technology (OT) environment, safety-critical infrastructure, and distributed systems that differ significantly from traditional enterprise IT environments.

The scope is expected to include, but not be limited to:

- Perform independent risk assessment, penetration testing and vulnerability assessment on NAS systems in accordance with FAA Orders, NIST guidance, and federal cybersecurity requirements.
- Conduct cybersecurity testing in lab, simulation, and operational environments while ensuring no impact to safety-critical NAS operations.
- Evaluate cybersecurity controls for operational technology, industrial control systems (ICS), SCADA systems, telecommunications infrastructure, and aviation-specific systems.
- Support regression testing and validation of remediation actions.
- Support NAS Cyber Operations (NCO) activities including threat hunting, incident response coordi-

nation, and development of Courses of Action.

- Support Tabletop Exercises and operational cyber response planning.
- Assess cybersecurity architecture of NAS systems including air-to-ground communications, radar, telecom infrastructure, cloud-integrated NAS systems, and hybrid legacy-modern environments.
- Evaluate system interdependencies across NAS operational, mission support, and R&D domains.
- Minimize the impact of cyber security events and incidents in support of availability and restoration requirements for NAS critical and essential services
- Assess current NAS cybersecurity posture, identify capability gaps and risks, evaluate emerging tools and techniques, and recommend improvements.

4. LOCATION OF WORK

The Place of Performance is at both Contractor and Government facilities, including FAA Headquarters (HQ) Washington D.C., FAA Air Traffic Control System Command Center (ATCSCC), William J Hugues Technical Center (WJHTC), FAA Telecommunication Infrastructure (FTI)/Harris Security Operations Control Center, Mike Maroney Aeronautical Center (MMAC), FAA Security Operations Center (Leesburg, VA), and Contingent Operations Locations.

5. NAICS CODE

The North American Industry Classifica-

tion System (NAICS) Code for this procurement has not yet been finalized.

6. Submittal Requirements for Market Survey

Interested sources should respond to this RFI/Market Survey by providing a Capability Statement in accordance with the requirements below:

One (1) cover page that includes:

- Name of the vendor/firm/corporation
  - Available NAICS, Unique Entity Identified (UEI) and CAGE code(s)
  - Business size and socioeconomic status
  - Point of contact (i.e., name, title, telephone, email)
  - FAA eFAST contract number (if available)

The Capabilities Statement (maximum of 5 pages including a cover sheet) should demonstrate

- A company's capabilities to perform cybersecurity work in NAS, aviation, or safety-critical environments.
- A company's experience performing the full work of work described in the SOW. The description must demonstrate your capability to perform work of similar size, scope, and complexity.
- A company's familiarity with FAA cybersecurity orders and NAS architecture.
- A company's ability to support Inde-

pendent Risk Assessments and Cybersecurity testing, at locations nationwide, on short notice.

- A company's ability to identify technologies, areas for development of new technologies, and analyze risks associated with each in order to mitigate vulnerabilities found in each risk assessment.

7. Other (if applicable)

Any proprietary or confidential information contained in the submission must be appropriately marked.

Contact Information

Primary Point of Contact

Elizabeth H. Williams

Email
eliza-beth.h.williams@faa.-gov
Phone Number
(blank)

Alternative Point of Contact

Stacy Roberson

Email
sta-cy.e.rober-son@faa.-gov
Phone Number
(blank)

Contracting Office Address

**15000 AVIATION BLVD., ROOM 5018
400W, 800 INDEPENDENCE AVENUE, SW
WASHINGTON, DC 20591 USA**

Attachments/Links

Links

No links have been added to this opportunity.

Attachments

Download All

Document	File Size	Acc
Attachment C SIR PA 25-080 91625.docx	189.81 KB	F