Open Architecture
Key Topics

Request for Information
70T04024I7573N001

April 26, 2024

Table of Contents

1.0 General Information 1
1.1 Introduction 1
1.2 Agency Name 1
1.3 Project Information 1
2.0 Background 1
3.0 Topic Areas 2
3.1 DICOS Image Data 3
3.2 Algorithm Development 5
3.3 Common Workstation 8
3.4 Threat Image Projection 9
3.5 Image Quality Standard 11
4.0 Disclaimer 11
5.0 Vendor Submission of Responses and Contact Information 12
6.0 List of Acronyms 14

Important Dates

Event	Date	Submission Requirements
Response to RFI	June 3, 2024, 12PM EDT	See Section 5.0 for details

1.0 General Information

1.1 Introduction

The Transportation Security Administration (TSA) is conducting market research to better understand vendor capabilities, qualifications, approaches, risks, and technical challenges with system components and subsystems of TSA's open architecture vision of a connected transportation security system of systems.

The information provided in this Request for Information (RFI) is subject to change and is not binding to TSA. All submissions become the property of TSA and will not be returned.

TSA is seeking information on multiple related topic areas from all interested parties, including, but not limited to, manufacturers, algorithm developers, and entities researching system components and subsystems. Respondents are encouraged to address all topic areas that are relevant to their organization.

1.2 Agency Name

Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive, Springfield, VA 20598

1.3 Project Information

RFI Number: 70T04024I7573N001
Project Name: Open Architecture System Components and Subsystems
Managing Program Office: Requirements and Capabilities Analysis in partnership with Acquisition Program Management and Information Technology Offices
Managing Program Division: Requirements, Human Performance, and Engineering Division

2.0 Background

The TSA's mission is to protect the Nation's transportation systems to ensure the freedom of movement for people and commerce. To achieve this mission in an evolving threat environment, TSA must prioritize being an agile and flexible organization which can rapidly field innovative screening solutions capable of improving TSA's security posture. Open Architecture (OA) is a design approach in which equipment components, such as software and hardware, are standards-based and interoperable to allow a wide range of industry partners to create improved subcomponents (like new detection algorithms, user interfaces, or reporting systems). TSA's OA vision is a connected transportation security System of Systems (SoS) in which state-of-the-art solutions are quickly adopted to address emerging threats and enables a dynamic screening environment.

In July 2023, TSA published two key documents that support TSA's OA initiative, the Administrator's Intent (Adm Intent) 3.0[1] and the TSA Open Architecture Roadmap[2] (Roadmap). The Adm Intent establishes OA as an agency priority, stating that TSA will "Develop and define common and accessible technical standards, capabilities, and processes to enable an open, streamlined, and secure infrastructure for transportation security screening." The Roadmap serves as a foundation for providing TSA's vision, goals, and objectives to establish a connected transportation security SoS.

TSA's OA methodology leverages standardized interfaces, data formats, communication protocols, and other appropriate solutions. Additionally, TSA is establishing framework, infrastructure, and toolsets to make TSA security screening data accessible, interoperable, and reusable by aviation security industry partners. To support this OA methodology, TSA will employ an agile approach in partnership with government and aviation security industry stakeholders.

TSA's approach allows a wide range of industry partners to create improved system components and subsystems, such as new detection algorithms, user interfaces, reporting systems, etc. These system components and subsystems will be interoperable within the transportation security SoS to allow TSA to quickly adopt state-of-the-art solutions to address emerging threats, and share information in real-time across screening solutions to enable a risk-based dynamic screening environment.

3.0 Topic Areas

TSA has defined multiple, concurrent initiatives that support system components and subsystems and provide enhancement of TSA's open architecture vision. This RFI is focused on the following:

- **Digital Imaging and Communications in Security (DICOS) Image Data** to include data collection; data standardization; data harmonization; image data annotation; data archiving, accessibility and distribution; and data maintenance.

- **Detection Algorithms** to enable rapid deployment and evaluation of enhanced and new anomaly and threat detection algorithms.

- **Common Workstations** to standardize the physical and graphical user interface across screening solutions to reduce training, certification, and complexity for TSA officers.

- **Threat Image Projection (TIP)** to support threat detection and mitigation using an artificial threat injection tool that projects images such as explosives, guns, knives, and other prohibited items in passenger bags or simulated bags on x-ray systems for Transportation Security Officers (TSOs) to adjudicate in an airport environment. TIP is intended to support vigilance during screening, exposure to emerging threats, performance measurement, operational testing, and research.

[1] Administrator's Intent 3.0, July 6, 2023, https://www.tsa.gov/sites/default/files/administrators_intent_3.0.pdf
[2] TSA Open Architecture Roadmap, July 31, 2023, https://www.tsa.gov/sites/default/files/oa_roadmap_20230717_508c-r1.pdf

- **Image Quality Standard** to establish a quality standard for images and an approach to evaluating the images and image metadata.

Respondents may provide information for one or more topic areas depending on their area of expertise. TSA is seeking responses from interested parties on the topic areas in this section to encourage industry engagement and ascertain market capability and capacity to meet the objectives of the Adm Intent and Roadmap. Respondents are encouraged to review TSA's Open Architecture Roadmap.

For all Topic Area Questions: TSA is interested in Respondent feedback on technical approach, risk mitigation, and schedule that can inform TSA's strategy for OA key topic areas. Respondents' answers should include the infrastructure, technology, and interface needs or assumptions to support their response.

The Respondents' answers should consider TSA's OA implementation strategy that includes leveraging the DICOS standard and Software Development Kit (SDK) and Open Platform Software Library (OPSL) SDK. Additionally, responses should consider TSA's IT environment and DHS/TSA cybersecurity requirements.

3.1 DICOS Image Data

Most algorithm development costs and resources are focused on up-front data collection and management. In response, TSA is implementing data collection, annotation, management, and distribution methodologies to provide industry partners with comprehensive and continuous data to support their algorithm development.

TSA is evaluating applying a data pipeline method to existing data collection and sharing initiatives. With a data pipeline method, up-front data collection decisions directly impact downstream utility of the data and vendors' ability to develop effective solutions in support of TSA's mission. This method will increase access to relevant data sets for all industry partners, allow for industry feedback and continuous improvement of data quality, improve solution performance, and reduce costs to TSA through a unified management approach. TSA will evaluate data classification and establish necessary policies to protect data privacy.

TSA has launched data collection initiatives across multiple capability areas. These initiatives support solution development, and TSA expects to expand these initiatives to ensure that data sets represent an operational environment. TSA will apply lessons learned to other capability areas as appropriate.

The focus of this topic area is on DICOS image data. TSA is seeking feedback to inform next steps for data management to include data collection, data harmonization, data annotation, data archiving and distribution as it relates to DICOS image data. Assuming solutions will be within the TSA IT environment, feedback should include what data is useful, how to make data available to industry and manage it going forward, and how to balance TSA's and vendors' needs.

Questions for Topic Area 3.1: DICOS Image Data

Overall Data Management

1. What demonstrated experience do you have performing DICOS image data collection? Please describe previous initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.

2. What demonstrated experience do you have performing DICOS image data harmonization to include homogenizing and organizing data, creating and building an information model, transforming data, data cleansing, and normalizing and classifying data? Please describe previous initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.

3. Describe your data management approach, to include identifying the differences in approaches for developmental data vs. testing data.

4. Describe your approach to data life cycle to include how long to keep data, when disposition should occur and how to validate that data is still relevant.

5. What risks or challenges do you see with TSA's planned DICOS image data pipeline method? How would you manage those risks? Please discuss experience and lessons learned.

6. Describe any other industries or programs doing similar work with image data to include what is working well and what is not.

7. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

Data Collection

8. What is your approach to DICOS image data collection to include planning, coordination, cybersecurity, transfer/submittal and overall program management?

9. Define your DICOS image data quality factors and outline your approach to data quality control and assurance.

10. What experience do you have working with and implementing the DICOS standard? Please describe initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

Data Harmonization

11. What is your approach to DICOS image data harmonization to include homogenizing, organizing, creating and building an information model, transforming, cleansing, normalizing, and classifying? Please describe your planning, coordination, cybersecurity, transfer/submittal and overall program management.

12. Define your DICOS image data quality factors for data harmonization and outline your approach to data quality control and assurance after data harmonization.

13. Describe techniques, tools, standards, and processes for validating data harmonization, including any challenges and lessons learned with the process.

14. Describe data harmonization initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

Data Annotation/Labeling

15. What is your approach to DICOS image data annotation, or labeling, to include methods, standards, and tools? Highlight any automation or efficiencies previously used or proposed to use for TSA efforts.

16. Describe tools, techniques, and processes for validating DICOS image data annotation used previously, as well as challenges and solutions applied to those challenges.

17. Define the timeframes for conducting all aspects of DICOS image data annotation for various data types (stream of commerce (SoC), explosive threats, prohibited items).

Data Archiving/Distribution

18. Describe your process for distribution and timeframes for each step involved in DICOS image data archiving and distribution (storage vs sharing). Discuss your internal processes and suggested approach to working within TSA's IT environment and supporting TSA's data repository.

19. What challenges do you anticipate and what solutions do you suggest for establishing a vetting process for individuals/companies regarding different levels of DICOS image data types?

3.2 Algorithm Development

The OA Roadmap outlines an objective to create a transparent and continuous mechanism to develop and evaluate solutions (like algorithms or workstations) while promoting market growth and competition. As part of the implementation of OA requirements, the TSA is moving towards an approach whereby system components and subsystems can be developed, tested, and deployed in accordance with TSA acquisition processes. This approach expands TSA's opportunities to partner with small and large businesses, public and private companies,

educational and research institutions, Federally Funded Research and Development Centers, and others. The ability to share data with common formats and interfaces in a unified way is an essential element of this approach.

Figure 1 shows a notional development and testing process for Automated Threat Recognition (ATR) algorithms. The notional process starts with developers leveraging DICOS and OPSL and includes TSA sharing various classifications of data with vetted industry partners. The data sharing would be governed by a data sharing policy outlining access levels and processes. TSA is considering an initial evaluation using an automated testing process under a vehicle that will encourage industry participation and also be cost effective for TSA. The results of the initial evaluation would inform the possible next steps of either further development or eligibility for a development contract with TSA (at TSA's discretion). Any ATRs deployed to an airport would have to undergo certification and lab and operational testing.

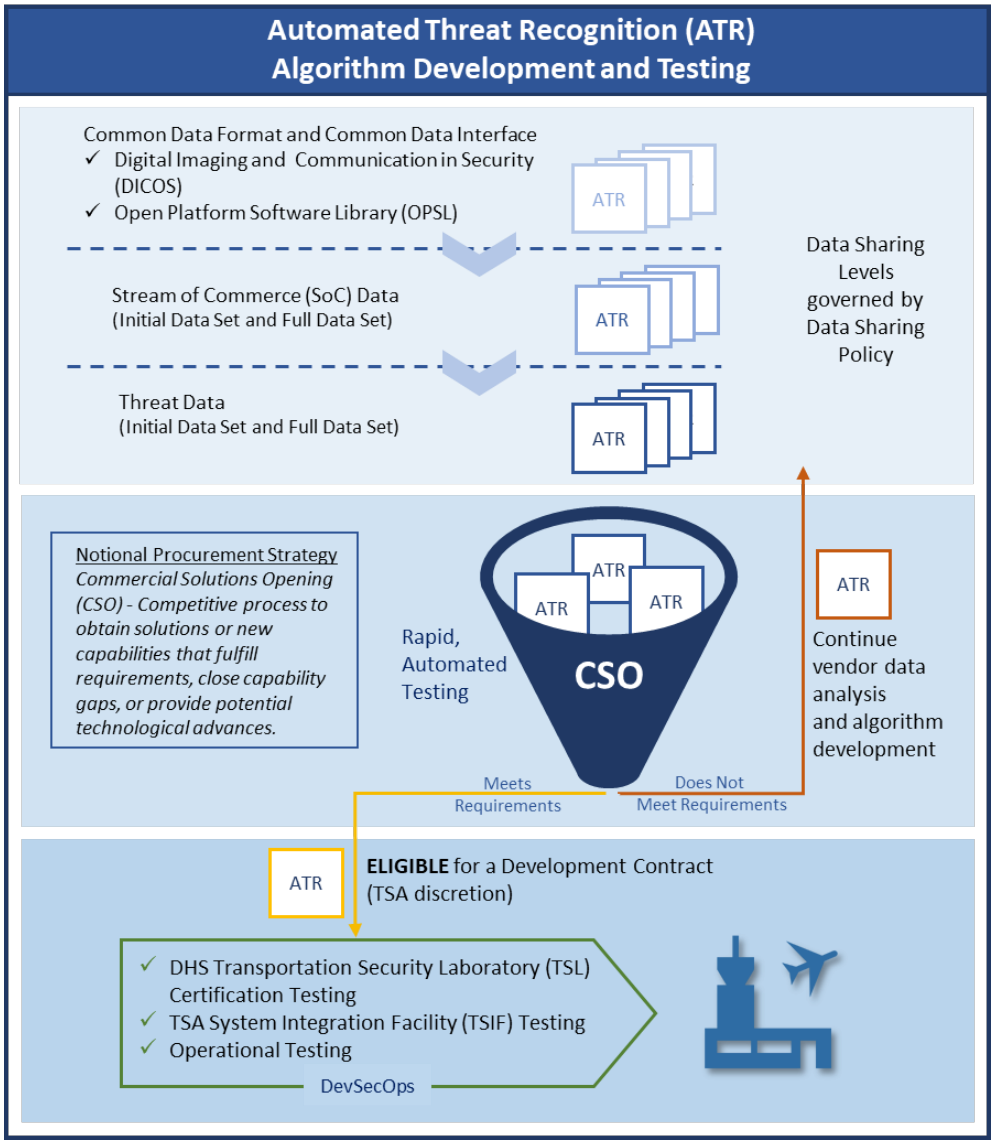

Figure 1. Notional Algorithm Development and Testing Process

Clear and consistent guidelines and processes will be essential to enabling rapid development and testing of solutions. TSA will outline the conditions in which developmental funding may and may not be provided to minimize technical and financial risks while promoting market growth and innovation. TSA aims to use robust data collection, annotation, and the management pipeline to promote continuous development and testing of OA solutions.

TSA is seeking feedback to inform its strategy and approach to develop and evaluate detection algorithms and to understand the current market.

Questions for Topic Area 3.2: Algorithm Development

1. What demonstrated experience do you have developing a detection algorithm? Please describe previous initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.

2. Describe your approach to modular coding techniques that has the flexibility to quickly add capabilities.

3. What aspects of algorithm development and testing are important to you and meet the needs of industry and TSA? Describe the risks and challenges associated with this effort.

4. Describe any other industries or programs implementing a similar development and testing process to include what is working well and what is not.

5. What data do you need and is most useful for algorithm development to include the amount of data needed and why, data categories, sensor data (concealment, orientation, etc.), and how the data is captured (voxel by voxel, etc.)?

6. Describe your capacity for conducting algorithm performance evaluations to include an integrated testing strategy to reduce time to test and deploy while ensuring high accuracy and detection performance.

7. Describe your capability and approach on how to protect data rights for non-government sponsored algorithms vs government sponsored algorithms. Describe how agreements can be used to ensure deeper understanding of how an algorithm works at the source code level while considering data rights/protections.

8. Describe your approach and capability to develop algorithms for one system/platform that can be applied to other systems and have the same or similar performance across all systems.

9. Describe any additional data needs from the system level other than what is outlined in DICOS v04[3].

[3] Digital Imaging and Communications in Security (DICOS) Information Object Definitions (IODs) (nema.org); September 29, 2023

10. Please identify any data gaps that you have by data category (SoC, military and commercial explosives, homemade explosives, prohibited items).

11. Describe your experience and approach to developing algorithm models that can be matured and trained with minimal turnaround time and cost efficiency.

12. What is the best way to leverage industry expertise for algorithm development while optimizing security and leveraging open solutions?

13. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

14. Provide recommendations on how TSA can develop a repeatable process to certify third party algorithms. Identify technical challenges and provide recommendations. Please comment on how the use of novel techniques (e.g. automated scoring, machine learning) can be leveraged to do algorithm scoring to reduce the certification workload while understanding that final certification needs to be performed in the "configuration intended to be deployed."

3.3 Common Workstation

The variety of transportation security equipment (TSE) in use has significantly complicated the TSA screening mission. This complexity is evident by the various user interfaces, training, and procedures required to utilize the different types of equipment. TSA aims to simplify technology and processes, standardize user interfaces, and rapidly respond to user needs. The ability to share data with common formats and interfaces in a unified way is an essential element of this approach. TSA's approach in which system components and subsystems can be developed, tested, and deployed in accordance with TSA acquisition processes further adds to TSA's need for a common graphical user interface (CGUI). While ensuring that the CGUI is consistent across technologies, as appropriate, it is priority that the CGUI maintain image quality standards and provide the image manipulation tools necessary to support the officer in conducting screening.

TSA has developed and demonstrated a Common Workstation (CW) that provides a CGUI that is connected and interoperable with TSE. TSA is seeking additional information from industry on a CW approach that uses a CGUI that supports the DICOS standard and OPSL middleware and can be integrated into TSA's transportation security SoS. Specifically, TSA is interested in a system that allows TSA to run different types of workstations/displays to include primary viewing stations used by officers to screen people and property, alternative viewing stations, and TIP management and reporting functions used by officers to resolve suspect items, supervisor workstations, and network stations. Additionally, TSA is interested in a training application that

leverages OPSL to enable TSA to train officers with a data set, and includes the ability for instructors/supervisors to recall, review and train on TIP images missed by officers.

TSA is seeking feedback to inform its strategy and approach to expand and implement a CW using a CGUI and to understand the current market.

Questions for Topic Area 3.3: Common Workstation

1. What demonstrated experience do you have developing a CW/CGUI? Please describe previous initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.

2. Describe your approach to taking a government defined interface standard and developing, testing and implementing a CW to include:

    - Use of commercial-off-the-shelf (COTS) products to the maximum extent
    - Software development
    - Testing environment
    - Zero Trust architecture principles
    - Modular code techniques that allow rapid capability improvement

3. Describe your capability to develop a standalone hardware/software that connects and interfaces with a "display" defined interface using OPSL and DICOS images created by Computed Tomography (CT), Advanced Imaging Technology (AIT), and other security technologies. Please include capabilities to provide image analysis tools and apply the solution to different screening levels and workflows.

4. Describe your capability and experience with rendering images with sufficient quality from a DICOS file.

5. Describe your capability and approach, to include the architecture, to take a government defined interface and expand the capability to support emulator development, testing and deployment to support detection algorithm evaluations.

6. Describe your approach to modular code techniques that has the flexibility to quickly add capabilities.

7. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

8. What is the source and formulas used to calculate your TIP provided reports?

3.4 Threat Image Projection

TSA's TIP program focuses the development, implementation, and maintenance of an artificial threat injection tool that projects images such as explosives, guns, knives, and other prohibited

items into passenger bags or simulated bags on x-ray systems for TSOs to adjudicate in an airport environment. The primary purposes of this tool are to support operator vigilance while conducting screening, to provide operators exposure to emerging threats, and as a detection performance measurement tool. Additionally, TIP can also supplement existing operational testing and TIP data can be used in research to identify detection trends, evaluation of new algorithms and programmatic opportunities (e.g., training).

TSA's OA initiative opens opportunities to expand and improve its implementation of TIP. A connected transportation security SoS using standard data and interface formats allows vendors, including small and large businesses, public and private companies, educational and research institutions, and Federally Funded Research and Development Centers, among others, to develop system components and subsystems.

TSA is seeking feedback to inform its strategy and approach to expand its TIP program and to understand the current market.

Questions for Topic Area 3.4: Threat Image Projection

1. What demonstrated experience do you have developing a TIP tool? Please describe previous initiatives to include the types of TIP images and the systems they were developed for, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.

2. Describe your approach and capability to develop DICOS TIP images and databases that can be used across different TSE. This includes "real images" (scanner collected) and generated images (e.g. synthetic data).

3. Describe your approach and capability to develop a vendor-agnostic inject tool that can be used across various types of screening technologies leveraging TSA OA solutions to include OPSL, DICOS, and the Threat Recognition System described in the OA Roadmap. Please include your approach to TIP management to include a scheduler, reporting, feedback loop, and updates.

4. Describe your approach to modular code techniques that has the flexibility to quickly add capabilities leveraging TSA OA solutions.

5. Describe your approach and capability to enable TIP to be leveraged by various TSA stakeholders (e.g., Testing, Training) for different purposes in a single, streamlined tool.

6. Describe your approach and capability to leverage OA solutions (ex., DICOS, OPSL) to enable TIP for various TSA stakeholders.

7. What experience do you have implementing cybersecurity requirements? Please describe initiatives, the scope of responsibility and expertise provided directly by your company, outcomes, and lessons learned.

8. Describe your approach and capability to collect data and develop TIP reports to be leveraged by airport officials and supervisors, to help optimize operational performance.

9. Describe your approach to implementing TIP network distribution across multiple primary viewing workstations to ensure consistent distribution of TIP images across active workstations.

3.5 Image Quality Standard

With connected, interoperable TSE and system components and subsystems that will use various hardware and software and perform image reconstruction and rendering, standardized and sufficient image quality is critical to ensuring consistent and optimized detection. TSA will need to establish a quality standard for images and image metadata, as well as an approach to evaluate image quality. This need applies to both images from screening systems and images displayed to officers for image interpretation.

TSA is seeking feedback to inform its strategy and approach for defining and enforcing image standards to include technical factors and challenges.

Questions for Topic Area 3.5: Image Quality Standard

1. Describe your capability and approach to evaluate TSE, system components, and subsystems' DICOS images to ensure consistent, quality images over time to support detection performance. Please include the hardware and software used to perform the evaluation.

2. Describe your capability and approach to develop requirements for TSE, system components, and subsystems that enables image quality evaluation and maintains high quality images to include automated tools.

3. Describe the technical factors and challenges that should be considered when establishing an image and image metadata quality standard and evaluation method.

4. Describe your capability to evaluate image quality at different stages (e.g., reconstruction, rendering, etc.).

4.0 Disclaimer

This RFI is issued for information and planning purposes only and does not constitute a solicitation. All information received in response to this RFI that is marked Proprietary will be handled accordingly. The Government will not return or pay for any information provided in response to this announcement; no basis for a claim against the Government shall arise as a result from a response to this notice or Government use of any information provided. Responders are solely responsible for all expenses associated with responding to this announcement.

The Government will review vendor responses for market research purposes only. The Government does not intend to provide a response to submissions for this RFI, but the Government reserves the right to hold a technical information exchange meeting with all, none or some of the submitters, after review of the RFI submissions, at the agency's discretion.

This RFI does not commit the U.S. Government to any course of action in the future. The Government will protect the information shared in the RFI response from disclosure to other parties. Each Respondent, by submitting a response to the RFI, agrees that any costs incurred in responding to the request or in support of activities associated with this RFI shall be the sole responsibility of the Respondent. The Government shall incur no obligations or liabilities whatsoever to anyone for costs or expenses incurred by the Respondent in responding to this RFI.

5.0 Vendor Submission of Responses and Contact Information

Interested parties are invited to submit a response. Respondents may provide information under any or all Topic Areas identified in Section 3.0.

Please provide written responses in either read-only Word or PDF format.

Questions concerning this RFI, should be emailed no later than May 17, 2024 at 12:00pm EDT to siobhan.mullen@tsa.dhs.gov and siobhan.lawson@tsa.dhs.gov. The subject line of the email should state, "Open Architecture Key Topics RFI 70T04024I7573N001 Questions - [Company Name]." Telephone inquiries will not be accepted or acknowledged, and no feedback or evaluations will be provided to companies regarding their submissions.

Written responses shall be submitted no later than June 3, 2024 at 12:00pm EDT to siobhan.mullen@tsa.dhs.gov and siobhan.lawson@tsa.dhs.gov. The subject line of the email should state, "Open Architecture System Components and Subsystems RFI 70T04024I7573N001 Response - [Company Name] [Email X of X]." It is the Respondent's responsibility to ensure the Government receives the Respondent's email submission.

Due to TSA restrictions on the size of email, ensure that all emails submitted are less than 5MB. If submissions exceed 5MB please divide into multiple emails. Any electronic submission determined to contain a virus will be deleted and not viewed. Facsimile and mail submittals will not be accepted. Do not use special characters in the file titles or provide files within files. Also, do not provide links within documents (for instance to a cloud sharing website).

The following sections provide a recommended outline for a response to this RFI. This outline is intended to minimize the effort of the respondent and structure the responses for ease of analysis by the Government.

Section	Content	Page Limit
Cover Page	Company's Name Company's Address Unique Entity Identifier (UEI) Company's Size and Socio-Economic Status information Contracting Points of Contact (Name, title, email, and phone number)	1
Executive Summary	Summarize key information from the submission to give the reader a brief overview. There should be no information in the Executive Summary that is not also elsewhere in the submission.	1
1: Corporate Expertise	Describe the company, products and services offered (commercial or not), history, ownership, and other information deemed relevant. Provide any past projects supporting TSA and a description of tasks performed. In addition, the respondent should include any relevant (similar in size, scope and complexity to the scope of work of this RFI) Government-wide Acquisition Contract (GWAC) held by the respondent. Include contract number, socio economic status, relevant NAICs, and period of performance.	2
2: Responses to Topic Area questions	Please respond to as many Topic Area questions as desired, identifying the Topic Area addressed. Feel free to present conceptual alternatives or innovations for concepts described in the Topic Areas. TSA encourages creativity, efficiencies, innovation, and alternate approaches to meeting TSA's mission. Individual Page Limits apply to each Topic Area	Topic Area 3.1 – 10 Topic Area 3.2 – 7 Topic Area 3.3 – 4 Topic Area 3.4 – 5 Topic Area 3.5 – 2
3: Feedback	Please provide any feedback on the elements in the proposed concepts, Sections 2.0 and 3.0, that are not clear or addressed within this RFI. Please explain what areas could be improved and why.	3

* Respondents should submit one response, regardless of number of Topic Areas addressed. Cover page, Executive Summary, and Sections 1 and 3, need only be provided once.

TSA-INSTR: NOTIFICATION TO OFFERORS OF CONTRACTOR SUPPORT OF RFI RESPONSES

Respondents are advised that employees of the firm identified below may review the RFI responses or provide other support in the RFI review process. This firm is expressly prohibited from competing on future subject acquisitions related to this RFI and from revealing respondents to anyone without a valid need to know.

Global Systems Technologies, Inc.
109 Floral Vale Boulevard Yardley PA 19067
POC: Chas McKee, 703-965-2209, chasm@gstpa.gov

In accomplishing their duties related to the review process, the aforementioned firm may require access to proprietary information contained in the Respondents' responses. Therefore, pursuant to FAR 9.505-4, in order to protect the Respondents' proprietary information, an agreement must be executed with the firm and each Respondent that states that the firm will: (1) protect the Respondent's information from unauthorized use or disclosure for as long as it remains

proprietary, and (2) refrain from using the information for any purpose other than that for which it was furnished. To expedite the process, each Respondent shall contact the above firm to effect execution of such an agreement prior to submission of responses. Each Respondent shall submit copies of the agreement with their RFI response.

6.0 List of Acronyms

Acronym/Abbreviation	Definition
AIT	Advanced Imaging Technology
ATR	Automated Threat Recognition
BAA	Broad Agency Announcement
BIC	Best in Class
CGUI	Common Graphical User Interface
COTS	Commercial Off-the-Shelf
CSO	Commercial Solutions Opening
CT	Computed Tomography
CW	Common Workstation
DevSecOps	Development, Security, and Operations
DICOS	Digital Imaging and Communications in Security
FAR	Federal Acquisition Regulation
GWAC	Governmentwide Acquisition Contract
IT	Information Technology
OA	Open Architecture
OPSL	Open Platform Software Library
RFI	Request for Information
RFP	Request for Proposal
SDK	Software Development Kit
SoC	Stream of Commerce
SoS	System of Systems
TIP	Threat Image Projection
TSA	Transportation Security Administration
TSE	Transportation Security Equipment
TSIF	TSA Systems Integration Facility
TSL	Transportation Security Laboratory
TSO	Transportation Security Officer
UEI	Unique Entity Identifier