Transportation
Security
Administration

Open Architecture Implementation

Request for Information
70T04023I7573N001

Version 1

February 2023

Table of Contents

Important Dates

Event	Date	Submission Requirements
Response to RFI	March 3, 2023, 3PM 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, costs, risks, and technical challenges with regard to TSA's vision of a connected transportation security system of systems based on open architecture principles and solutions.

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, integrators, and entities researching system components and subsystems. Respondents are encouraged to address any of the topic areas that are relevant to their organization. Agency Name

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

1.2 Project Information

RFI Number: 70T04023I7573N001
Project Name: Open Architecture Implementation
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

2.1 Current State

TSA's mission is to protect the nation's transportation systems to ensure the freedom of movement for people and commerce. TSA is challenged with the need to establish a solution for 55,000 officers who screen over 2 million passengers, on average, per day at over 430 federalized airports with nearly 1,500 checked baggage systems and 680 checkpoints with 2,360 lanes. The current screening system is highly complex, with limited standardization of data and interfaces. The lack of standardization limits TSA's ability 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. It also puts an ever-increasing burden on TSA's frontline officers to perform the critical screening function with cumbersome procedures, complex training, and varied user interfaces.

Currently, TSA relies exclusively on Original Equipment Manufacturers (OEMs) of Transportation Security Equipment (TSE) for upgrades. As TSA continues to mature the security screening process, it needs to leverage industry partnerships and expand engagement with innovative solution providers like small businesses and academic institutions, while maintaining

relationships with OEMs to provide best-in-class security for our frontline officers and the traveling public.

2.2 Future State Vision

To achieve TSA's mission in an evolving threat environment while continuing to provide efficient screening solutions that support the frontline officers securing the transportation system and enhance the passenger experience, TSA prioritizes being an agile and flexible organization that can rapidly field innovative screening solutions. In addition, TSA seeks to enhance industry partnerships that allow adoption of increasingly interconnected and interoperable technologies while employing advanced cybersecurity capabilities.

TSA's vision is a connected transportation security system of systems in which state-of-the-art solutions are quickly adopted to address emerging threats and enable a dynamic screening environment.

A system of systems is defined as a set of systems or system components that interact to provide a unique capability that cannot be accomplished independently. The key to achieving TSA's vision of a superior transportation security system of systems is an open architecture design approach where components are standards-based and interoperable. This vision supports TSA's commitment to our most important asset, the dedicated frontline officers securing the transportation system, by providing the best tools to conduct mission critical screening operations while simplifying operational processes and procedures. TSA leverages the following open architecture principles to guide initiatives and realize the desired end-state:

- **Standardization:** Implement and maintain standardized interfaces, data formats, and other solutions in an intentional and agile approach in partnership with government and industry stakeholders.
- **Open Data:** Establish open, high-quality, comprehensive datasets available to transportation security industry partners.

These open architecture guiding principles allow a wide range of industry partners to create improved subcomponents, such as new detection algorithms, user interfaces, reporting systems, etc., that can be interoperable within the transportation security system of systems 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.

2.3 Initiatives and Activities

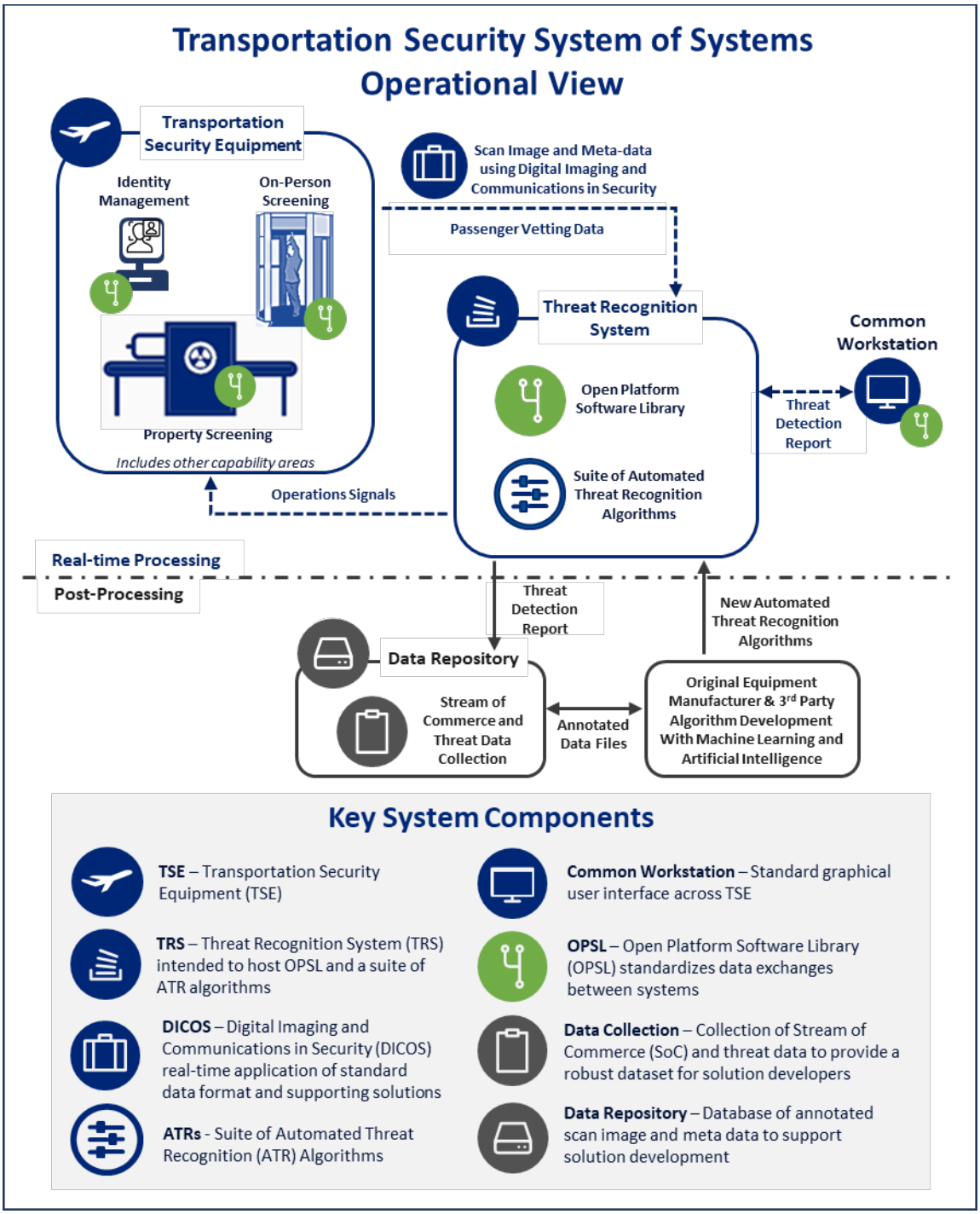
TSA has defined multiple, concurrent initiatives that implement open architecture principles to establish a connected transportation security system of systems. This RFI is focused on the following:

- **Common** data formats and interfaces to facilitate interoperability:
  - Digital Imaging and Communications in Security (DICOS): development of the standardized data format (DICOS v3.0+) and associated toolkits for capturing data and providing it in a non-proprietary format.

  - Open Platform Software Library (OPSL) Development: standardizes data exchanges within systems to enable communication of mission data between system components.

- **Data accessibility** to establish a comprehensive dataset that can be used to capitalize on industry advancements in artificial intelligence, machine learning, and other solution development. Industry guidance indicates that the majority of algorithm development effort is focused on the up-front data collection and management.
  - Stream of Commerce (SOC) and Threat Data Collection: collects and documents passenger baggage images and associated metadata in an efficient manner.
  - Passenger Baggage Object Database (PBOD) Establishment: stores and catalogs threat and SOC data in DICOS format in a data repository to support sharing with industry partners and government test facilities.
- **Common Workstation** to standardize the physical and graphical user interface across screening solutions to reduce training, certification, and complexity for the officers.
- **Threat Recognition System** (TRS) construct to combine computing hardware, OPSL, and DICOS into a platform supporting interoperable screening equipment (on-person, accessible property, etc.) while decoupling the algorithm and Common Workstation through vendor-neutral Application Programming Interfaces (APIs) and communication protocols.

The role of these initiatives in the future transportation security system of systems is illustrated in the figure below.



TSA has completed a number of activities and is planning many more that support the initiatives implementing open architecture principles. Achievements to date include publishing the DICOS v3.0 standard and associated toolkits in partnership with the National Electrical Manufacturer's Association (NEMA) and industry stakeholders, releasing to industry the initial version of the OPSL Software Development Kit (SDK), and completing TRS design reviews and prototype development to enable future laboratory and field demonstrations.

3.0 Topic Areas

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 achieve the desired objectives outlined under the topic areas. TSA is also interested in Respondent feedback on technical approach, risk mitigation, cost, and schedule that can inform TSA's transportation security system of systems implementation strategy. Respondents may provide information for one or more topic areas depending on their area of expertise.

3.1 Common and Accessible Data Formats and Interfaces

TSA has been collaborating with NEMA and industry stakeholders for more than a decade to develop the DICOS standard for security screening images and related data. The DICOS standard facilitates the creation of a connected transportation security system of systems with a common and accessible data format.

Building on the success of DICOS as a standardized data format, TSA, in collaboration with industry, has produced the first iteration of the OPSL to provide a common middleware service to enable standardized communication protocols and APIs. The OPSL standardizes how software interacts with other software to support interoperability between screening solutions and secure information exchange of scanner images, Threat Detection Reports (TDRs), and other critical mission data.

TSA has developed and released DICOS SDK for each DICOS version to support consistent implementation of the DICOS standard across vendor solutions. The OPSL SDK is also available at no cost to support vendor development, testing, and implementation.

As TSA expands OPSL and DICOS implementation, the OPSL SDK and DICOS SDK will transition to user-driven software projects to ensure end-user usability, solution transparency with approved parties, and improved speed and quality in the development, testing, and maintenance of the solutions. TSA views a future where the OPSL SDK and DICOS SDK are maintained and matured through a collaborative effort with industry, with TSA providing only the level of governance and facilitation needed to ensure releases are available to TSA's industry partners.

In this model, TSA will facilitate which features and updates are prioritized and approved, coding best practices and quality, and cyber security standards. Industry partners will have access to the source code, propose and develop improvements at their pace, and implement improvements in coordination with TSA.

The user-driven model enables TSA to leverage open-source software development methodologies and industry best practices and talent to continuously develop, test, and maintain the OPSL SDK and DICOS SDK long-term. Additionally, a user-driven model provides industry with maximum code transparency to adapt their capabilities to be compliant with open architecture principles, and code can be improved at a tempo consistent with TSA's mission and industry needs.

TSA expects products to be developed within a Development, Security, and Operations (DevSecOps) methodology. DevSecOps adds security design to the DevOps software development and operations process through a collaborative approach to integrate security by design, testing, and integration early and throughout the development and deployment lifecycle rather than waiting at the end to insert security measures at the time of deployment. DevSecOps enhances TSA's capability to manage and maintain the release of software while maintaining or improving quality and the capability to scale agile production and test without compromising system security. Additionally, DevSecOps approaches and methods quickly and efficiently purge technical debt (accumulation of non-compiled code) and detect and respond to software anomalies and flaws during production and real-time operations.

TSA is seeking feedback to inform next steps for standardized data format and interface implementation, including how to make source code available to industry and manage it going forward, how to create pathways for feedback, and how to balance TSA's and vendors' needs.

Questions for Topic Area 3.1:

1. Do you have experience with open standards-based software development through APIs and codes designed to securely permit communication and share data between applications in a unified way? Please describe previous initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned. Lastly, indicate the current state of your company's capabilities for initiatives described above.
2. What experience do you have working with and implementing the DICOS Standard? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
3. What demonstrated experience do you have with developing, utilizing, tailoring, or otherwise working with multiple SDKs? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
4. What demonstrated experience do you have with agile software development? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
5. What demonstrated experience do you have with software factory methods, including containerized micro services with mutable infrastructure and build in security? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
6. What experience do you have with verifying compliance for common and accessible data formats and interfaces?
7. What is your approach to working with and managing user-driven software solutions?
8. How does your organization implement DevSecOps and what is its maturity level?
9. What are the challenges you have experienced when practicing DevSecOps software development and delivery? How did you resolve/address those challenges?

10. How would you manage government and industry (e.g. OEMs, 3rd party, academia, or national lab) requirements intake, prioritization, and implementation for each SDK?
11. How would you manage release schedules, version control, configuration management for interface components, software configuration management processes, and implementing a Continuous Integration and Continuous Deployment/Delivery (CI/CD) infrastructure overall?
12. What are your Cyber Security and Cyber Risk Management qualifications? Please describe any Cyber Security certifications.
13. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
14. What feedback or industry best practices would you provide to enable transition of the OPSL SDK and DICOS SDK to a user-driven model?
15. What user-driven models do you have experience with for maintaining open architecture standards? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
16. What risks or challenges do you see with TSA's planned approach? How would you manage those risks? Please discuss experience and lessons learned.

3.2 System of Systems Implementation

A successful transportation security system of systems approach will define an integrated environment that promotes maximum interoperability. In partnership with stakeholders, TSA will define the intermediate and long-term integrated transportation security system of systems environment. With multiple viewpoints and approaches, it is essential that TSA proactively document, analyze alternatives, and implement incremental solutions while working towards long-term goals.

This RFI focuses on TSA's concept of the TRS, which combines the computing hardware, DICOS, and OPSL, to provide a common computing platform supporting interoperable screening equipment and enables the ability to leverage multiple industry partner algorithms, Common Workstations, and other innovative solutions. The TRS approach mitigates potential cyber security vulnerabilities by providing a common operational solution to minimize the threat space and improve the ability to mitigate emerging cyber threats. TSA aims to leverage the concept of Operational Technology (OT) for screening systems which requires different cyber approaches than standard Information Technology. TSA will include Zero-Trust approaches as well as a real-time capability to isolate cyber vulnerabilities in a connected transportation security system of systems so that screening operations can continue securely.

DICOS and OPSL have been successfully tested with multiple vendors. TSA has a prototype TRS consisting of OPSL and a suite of Automated Threat Recognition (ATR) algorithms based on DICOS 3.0+ currently in place at the TSA Systems Integration Facility (TSIF). The first laboratory demonstrations of a working, full-scale TRS integrating Computed Tomography (CT)

and Advanced Imaging Technology (AIT) scanners with a common workstation are planned to occur in FY23, and are expected to be followed by larger field demonstrations at airports. These demonstrations will help TSA evaluate performance, functionality, and scalability while establishing a cost-effective and sustainable deployment strategy.

TSA will intentionally sequence laboratory and field demonstrations to allow for an iterative approach to discover and correct issues with minimal impact on checkpoint operations while reducing overall technical and programmatic risk, which will enable scaling solutions at a later date.

TSA expects to mature and evaluate TRS concepts in partnership with industry stakeholders for select capability areas prior to scaling to additional solution types.

TSA anticipates using a systems integrator to manage the TRS prototype and its interoperability with other system components, and to coordinate with vendor and airport stakeholders during these maturation activities. TSA is seeking feedback to inform the approach to conduct field demonstrations of complex, open, and connected system of systems.

Questions for Topic Area 3.2:

1. What qualifications and experience do you have as a systems integrator in an airport environment or similar? Please include a detailed description of your specific qualifications, capabilities, processes, procedures, tools, and successfully completed system integration efforts (including scope/magnitude of each effort, and how cost, schedule, performance, risks/issues, quality, development, testing, configuration management, physical space limitations and security, integration, deployment, retrofitting, and maintenance of operational technology software, hardware, and network components were managed and implemented). Include details about infrastructure and installation coordination with different entities to include meeting local requirements such as but not limited to permitting, power availability, and seismic considerations (as applicable).
2. What experience do you have in scaling systems to accommodate increasing capability needs? What specific approaches, processes, procedures, and tools have you used for scaling systems? Please include lessons learned that may help shape the direction of the open architecture implementation.
3. What demonstrated experience do you have maintaining open architecture systems using software factory methods, including containerized micro services with mutable infrastructure and build in security? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
4. What specific challenges have you experienced in managing systems integration efforts? How did you address those challenges? What were the outcomes? What were the lessons learned?
5. What specific experience do you have in managing system transition activities – including transition planning, procurement of tools and equipment, multi-vendor coordination, and transitioning prototype systems to fully interoperable deployed systems? Please describe initiatives, outcomes, and lessons learned.

6. What is your approach to managing stakeholder relationships and communications to support systems integration activities?
7. What is your approach to protecting Intellectual Property (IP) and avoiding conflicts of interest in a system of systems environment? Please describe any challenges or considerations.
8. How would you manage government and industry (e.g. OEMs, 3rd party, academia, or national lab) requirements intake, prioritization, and implementation for systems integration efforts?
9. How would you manage release schedules and version control for software, hardware, and network components that conform to the open standard? How would you address configuration management processes for overall system components, configuration items, IT assets, change parameters, and software?
10. With consideration for a system of system, please discuss your recommended approach for a Test & Evaluation (T&E) strategy to include the development environment as well as the formal Developmental Testing and Operational Testing phases of the acquisition program. How would you approach the testing and evaluation of the system of system, sub-systems, components and equipment in each of these environments/phases? Please include your approach to preferred testbeds for software and hardware, documentation and reporting methods, test management systems, configuration management, third party testing, certification, test sequencing, dual use/integrated testing as well as vendor and government responsibilities.
11. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
12. What industry best practices do you use to ensure systems integration efforts are efficient, effective, and optimized?
13. What risks, issues, or challenges do you perceive with TSA's planned systems integration approach? How would you manage those risks, issues, or challenges? Please discuss your experience, lessons learned, and any proposed alternative design concepts which could reduce systems integration risk overall.
14. What specific acquisition, maintenance, and procurement strategies would you recommend to support TSA's planned system of systems approach?
15. How would you identify the sub-systems and assign performance requirements within the system of systems? Are there specific components or equipment which should be maintained as a unit and not separated as distinct sub-systems? Why? What level of detail is required for integration requirements?

3.3 Enabling Subsystem and Component Development

As part of the implementation of open architecture requirements, the TSA is moving to a new approach where subsystems and components can be developed, tested, and deployed by vendors in accordance with TSA acquisition processes, including small and large, public and private

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

TSA has instituted holistic and continuous data collection, annotation, management, and distribution methodologies and solutions to enable solution development and testing with industry partners. Ongoing data collection initiatives have captured scanner images and associated data in DICOS format that TSA aims to share with vetted industry partners to support solution development.

TSA is interested in feedback on ways to provide access to these datasets that support TSA's and vendors' needs. The goal is to maximize innovation in solution development through effective data sharing that supports industry partner efforts. Responses to this topic area should focus on mechanisms for data sharing, and not on how data was used to develop a product.

Questions for Topic Area 3.3:

1. What is your approach to utilizing common interface standards for modular systems and components as it applies to cyber security applications? Please address those that apply to hardware interfaces, communication protocols, and data formats for data to be securely exchanged between different systems.
2. What experience do you have in facilitating data sharing agreements to support applications development? Please describe the type of agreement or provide samples, the type of data, data transfer method, any applicable data conversion tools utilized, and constraints on data use.
3. What experience do you have working with different entities that develop subsystems and components to integrate to an established ecosystem? Describe the approach and experience from providing oversight and expertise for requirements development, documentation, and compliance.
4. Have you experienced issues with developing common data formats to share data between applications in a unified way, related to specific clauses or the lack of clauses addressing situations that arose? Please describe the situation and how you would do differently to avoid the resulting issues.
5. What experience do you have managing DevSecOps software factory development practice that results in delivering software applications and system components quickly and frequently? Please describe your approach in software containerization, micro-services, building in security, structuring repeatable and defined paths to create, update, and test software applications and system components that use the software.
6. Describe your experience or approach to enable industry access to government systems and data. Include experience and knowledge in obtaining critical approvals such as but not limited to Authority to Operate (ATO). Describe your approach to provide access to datasets in those systems.

7. What experience do you have implementing cyber security requirements? Please describe initiatives, the scope of responsibility and expertise supplied directly by your company, outcomes, and lessons learned.
8. How would you address configuration management (hardware and software) for modular system components, associated software configuration management processes, and implementing a Continuous Integration and Continuous Deployment/Delivery infrastructure for modular components overall?
9. What feedback or industry best practices would you suggest to optimize DevSecOps software factory development practice and mitigate risks and issues?

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.

This RFI does not constitute a Request for Proposal (RFP) or any commitment or intent to issue an RFP, Broad Agency Announcement (BAA), or solicitation. This RFI does not commit TSA to contract for any supply or service. TSA is not seeking proposals at this time. Responders are advised that TSA will not pay any costs incurred in response to this RFI. All costs associated with responding to the RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future solicitation.

The information provided in this RFI is subject to change and is not binding on TSA. All submissions become the property of TSA and will not be returned. Additionally, it should be noted that TSA is requesting information on this topic to identify various solutions to support open architecture that are currently available or being developed.

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. Respondents only need to submit the information in Section 1, 3, and 4 below once regardless of the number of Topic Areas addressed in the response.

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

Written questions concerning this RFI, should be emailed to siobhan.mullen@tsa.dhs.gov and siobhan.lawson@tsa.dhs.gov no later than 3:00pm EDT, February 20, 2023. 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 Friday, March 3, 2023 at 3:00pm EDT to siobhan.mullen@tsa.dhs.gov and siobhan.lawson@tsa,dhs.gov. The subject line of the email should state, "Open Architecture Implementation RFI 70T04023I7573N001 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) Number 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 vendor or respondent should include any Government-wide Acquisition Contract (GWAC) details (regardless of Best In Class (BIC) status) it holds, including the contract number, small business category, title, and period of performance. For instance, if the vendor has a GSA Multiple Awards Schedule this information should be in the RFI response as well. The GWAC should be applicable to the scope of work stated in this RFI.	2
2: Responses to Topic Area questions	Please respond to as few or 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	10 per topic area

Section	Content	Page Limit
3: Experience	Describe three (3) key projects the company has participated in that are similar in size, scope, and complexity to TSA's environment. Briefly describe the customer environment, application solution designed/implemented, project management methodology, security requirements, best practices implemented, and relevant lessons learned. Describe any certification and accreditation processes for systems to achieve an ATO.	3
4: Questions and Feedback	Please provide any questions or feedback on the elements in the proposed concepts, Sections 2.0 and 3.0, that are not clear within this RFI. Please explain what areas could be improved and why.	3

This RFI is issued solely for market research, planning, and information purposes in order to assist TSA. 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.

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
109 Floral Vale Boulevard Yardley PA 19067
POC: Chas McKee (703-965-2209)

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, these firms must execute an agreement with each Respondent that states that they 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 company 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 (millimeter wave)
API	Application Programming Interface
ATO	Authority to Operate
ATR	Automated Threat Recognition
BAA	Broad Agency Announcement
BIC	Best In Class
CI/CD	Continuous Integration and Continuous Deployment/Delivery
CT	Computed Tomography
DevSecOps	Development, Security, and Operations
DICOS	Digital Imaging and Communications in Security
FAR	Federal Acquisition Regulation
NEMA	National Electrical Manufacturer's Association
OEM	Original Equipment Manufacturer
OPSL	Open Platform Software Library
OT	Operational Technology
PBOD	Passenger Baggage Object Database
RFI	Request for Information
RFP	Request for Proposal
SDK	Software Development Kit
SOC	Stream of Commerce
T&E	Test & Evaluation
TDR	Threat Detection Report
TRS	Threat Recognition System
TSA	Transportation Security Administration
TSE	Transportation Security Equipment
TSIF	TSA Systems Integration Facility
UEI	Unique Entity Identifier