U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

To be posted under the Transportation Security Administration's Open Architecture Initiatives
SAM Notice ID: TSA25-04-03789

I. Purpose:

The Transportation Security Administration (TSA) is posting this announcement to provide interested entities an opportunity to obtain access to information (up to Sensitive Security Information (SSI)) regarding the next generation Open Architecture (OA) solutions and applications.

The goal of sharing this information is to provide industry an understanding of the next generation OA solutions and applications and enable them to provide feedback to TSA. Industry feedback will help TSA understand industry capability and product development for OA solutions and applications and allow TSA to gauge viability of future Open Architecture requirements. Industry feedback received early in the planning and development process will provide TSA necessary information for decision making. Additionally, industry feedback may identify opportunities for Industry to participate in non-funded OA proof-of-concepts/demonstrations of prototypes that work with TSA Open Architecture solutions.

II. Applicability

Receipt of the OA SSI is limited to (a) current OA Solutions/Application developers/manufacturers; (b) potential OA Solutions/Application developers/manufacturers; and (c) third-party organizations with relevant experience in OA solutions/applications development and integration.

SSI information includes:

- Draft requirements that provide an indication of targeted performance for user assisted capabilities;
- Transportation Security Equipment (TSE) Common Graphical User Interface (CGUI) Specifications;
- Operational performance metrics for detection algorithms;
- Threat Recognition System (TRS) specifications; and
- Computed Tomography (CT) images in Digital Imaging & Communications in Security (DICOS) v02a format.

III. Instructions

For Non -SSI OA information, such as the Open Platform Software Library (OPSL) Software Development Kit (SDK)and DICOS SDK, which can be run in a virtual set up, vendors may request access by emailing OAsupport@tsa.dhs.gov. For SSI OA information as referenced above:

A. Entity Responsibility.

B. Senior Corporate Official. Each entity with individuals requesting access to SSI, shall designate a single, corporate official who will serve as the point of contact for all individuals of that entity

requesting sensitive information. The Senior Corporate Official will ensure that a notification is sent to OASupport@tsa.dhs.gov when individuals no longer require access to SSI. If additional individuals of the entity need access to this SSI, they must follow the procedures listed within this notice.

C. Criteria for Release. As part of this release, SSI may only be accessed by individuals who have successfully passed a Security Threat Assessment. This assessment may include a verification of site facility clearance in the National Industrial Security Program (NISP), contractor suitability determination or other federal background investigation, individual security clearance(s), and if required, a criminal history records' check (CHRC) and/or a check against terrorism or other databases. At no point shall any SSI provided be copied, duplicated, forwarded or shown to any individual not approved by the TSA.

D. Information Requirements. Consistent with the criteria for release described above, the requester's Senior Corporate Official must provide the appropriate information to the TSA as identified below. Note that this requirement applies likewise to any prospective subcontractor, joint venture partner, or "team" company who will have access to the specified SSI. All information must be emailed to OASupport.tsa.dhs.gov. with the subject line "OA Information Request – *[insert entity name]*" This information will be handled in accordance with the applicable Privacy Act System of Records Notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS), noted in Paragraph F, below.

1. Entity's System for Award Management (SAM) Unique Entity Identifier (UEI), the CAGE code of the entity's facility that will manage the SSI, Dun & Bradstreet Tax Identifier (ID) Number, and entity's address. TSA may review reports from these systems/sites to ensure the requesting corporate entity would not otherwise be precluded from partnering with the Federal Government. However, access to this SSI is not tied to a solicitation and authorization for access to the SSI is at the discretion of the TSA.

2. Name, title, phone number, and email address for the entity's designated Senior Corporate Official. This individual must certify in writing: 1) only authorized individuals will have access to sensitive information, 2) those authorized individuals adequately understand their responsibilities to protect this information, and 3) all appropriate protections will be followed in receiving and maintaining the SSI information.

3. A paragraph indicating the need to know for the SSI information and how the requests apply to the Open Architecture effort.

4. List of projects relevant to OA that have been successfully completed, and/or OA related research papers that they have authored. Either shall be accompanied by a short summary with any additional, relevant information in regard to Section II above. The total page count for the list, research papers, and/or relevant information shall not exceed one page.

5. For all employees who are requesting access to SSI, the following information shall be provided in a single password protected Microsoft Excel spreadsheet. The single password for the protected Microsoft Excel spreadsheet shall be sent to the OASupport@tsa.dhs.gov in a separate email, at the same time. This spreadsheet shall include:

- Employee Full Name
- Employee Birth Date
- Employee Citizenship
- Whether requesting employee:
  - Previously underwent a federal background investigation with TSA or other federal entity; or
  - Possesses an individual security clearance, or
  - Previously received authorized access to SSI.

While not required in the original information provided by the Senior Corporate Official, it should be noted that in rare instances Social Security Numbers may be required for individuals requesting access to SSI. In those instances, the Senior Corporate Official will receive an email from OASupport@tsa.dhs.gov requesting the Social Security Number for those individuals. The Senior Corporate Official shall provide the requested information back to OASupport@tsa.dhs.gov in a password protected document using the same password used and provided for the protected Microsoft Excel spreadsheet.

E. Non-Disclosure Agreements. Each individual requesting access to SSI as specified herein will be required to execute a Non-Disclosure Agreement (DHS Form 11000-6). The executed forms shall be provided as part of the submission of information reflected in Paragraph D above. The requester should understand that individuals granted access to SSI and signing a Non-Disclosure Agreement are bound by the terms of that Agreement indefinitely, notwithstanding their employment status or any other background checks or clearances granted by any Government agency. Additionally, submission of a Non-Disclosure Agreement for this request does not substitute for required NDAs required later by TSA.

F. Privacy Act Statement. The TSA will use the information provided by requesters to conduct a security threat assessment on individuals who seek access to SSI. The information provided by the requesters will be shared within DHS with personnel who need the information to perform their official duties. Additionally, DHS may share the information with law enforcement, intelligence, or other government agencies as necessary to identify and respond to potential or actual threats to transportation security in accordance with the routine uses identified in the applicable Privacy Act System of Records Notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on August 11, 2014, and can be found at 79 FR 46862-46866. Authority: 49 USC 114. Furnishing this information is voluntary. However, failure to furnish the requested information may delay or prevent the completion of a security threat assessment, without which an individual may not be granted access to the SSI.

G. Notification of Assessment. If it is determined that a requesting individual is not eligible to receive access to this SSI based on the Security Threat Assessment, the TSA will provide the entity's Senior Corporate Official notification that the individual does not qualify to receive SSI. Appeal of the determination will not be permitted due. However, the entity may nominate another individual to receive SSI access. In the event that an individual is not eligible to receive access to this SSI based on the Security Threat Assessment and the individual believes that the results of the vetting are inaccurate, he or she may request access to their records by submitting a Privacy Act Request

through TSA's Freedom of Information Act (FOIA) internet site at: https://www.tsa.gov/foia/requests.

IV. Once Approved

1. Draft requirements, applications, and data can be provided and received electronically by entities in accordance with SSI procedures.

2. To obtain the CT images in DICOS v02a format, entities must provide an encrypted hard drive with 5TB of storage space. A list of the acceptable models of encrypted drives that must be used will be provided.

3. Return of SSI. Any SSI must be returned to the Government if requested. The Government will verify that all requested SSI has been adequately returned. For instance, the Government may ask for deletion of the SSI data and the vendor will be required to delete all data and provide proof to the Government. All removal and return of data shall follow SSI guidance. Industry guidance can be found in https://www.tsa.gov/for-industry/sensitive-security-information.

V. Submission

Requests for OA SSI access with the required information as listed above and summarized in the following table shall be submitted electronically to the following email addresses: OAsupport@tsa.dhs.gov no later than **2:00 PM EST on February 28, 2025.**

Description	Format
Entity's SAM UEI, the CAGE code of the requester's facility that will manage the SSI, company address, and company Tax ID Number per Section III.D.1.	Email submitted by Senior Corporate Official
Senior Corporate Official's name, title, phone number, and email address per Section III.D.2.	Email submitted by Senior Corporate Official
A paragraph indicating the need to know for the SSI information and how the requests apply to the Open Architecture effort per Section III.D.3.	Email submitted by Senior Corporate Official
OA related projects, papers, etc. per section III.D.4.	Attachment to Email above - Microsoft Word or Adobe PDF
Representative Vetting Information See Section III.D.5.	All requesting individuals' information in one Attachment to Email above - Password Protected Microsoft Excel followed by email with Password
Non-Disclosure Agreements initialed and signed by requesting individual and signed by witness per Section III.E.	Attachments to Email above – DHS Form 11000-6 for all requesting individuals

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598