Transportation Security Administration (TSA)

Qualified Products List (QPL)

Checkpoint Property Screening System (CPSS)

QPL Overview

70T040CPSSQPL

October 04, 2019

Checkpoint Property Screening System (CPSS) Qualified Products List (QPL) Overview

1.0 Introduction

The Transportation Security Administration (TSA) has found that the most impactful technology available to address the rapidly-evolving threats in airport checkpoints today is Computed Tomography (CT). Therefore, TSA intends to establish the Checkpoint Property Screening System (CPSS) Program to qualify CT systems for use at airport passenger screening checkpoints nationwide. For the CPSS Program, TSA will apply an incremental approach to rapidly deploy this new technology. TSA will evolve the CT technology to meet its mission by continuing to work within the trade-space established by the thresholds and objectives defined in the Accessible Property Screening System (APSS) Operational Requirements Document (ORD). Incremental enhancement occurs when an additional discrete segment of capability is tested and approved for installation and deployment on TSA's CT system fleet. For each increment, TSA intends to establish updates to the existing CPSS Functional Requirements Document (FRD) that speaks to the area within the trade-space that meets the incremental enhancements acceptable baseline. CPSS incremental enhancements will be rolled out throughout the program and adhere to updated functional requirements that are traceable to the APSS ORD.

1.1 Establishment of the CPSS Qualification Process

TSA is establishing a Qualification Process for CPSS in accordance with the requirements of Federal Acquisition Regulation (FAR) 9.202. The Qualification Process is the means by which products are provided by the QPL Applicant in order to test the submitted product performance against the CPSS requirements. The purpose of this overview notice is to notify industry that TSA is initiating the CPSS qualification process.

TSA has no limitations concerning who may submit as a QPL Applicant in the CPSS Qualification Process and QPL Applicants are not required to be the Original Equipment Manufacturer.

Figure 1 below, titled "Qualification Process", provides an overview of the steps in the Qualification Process. The Qualification Process is also described in the Qualification Management Plan (QMP). This Qualification Process may be tailored for the needs of a QPL Window as determined necessary by TSA.

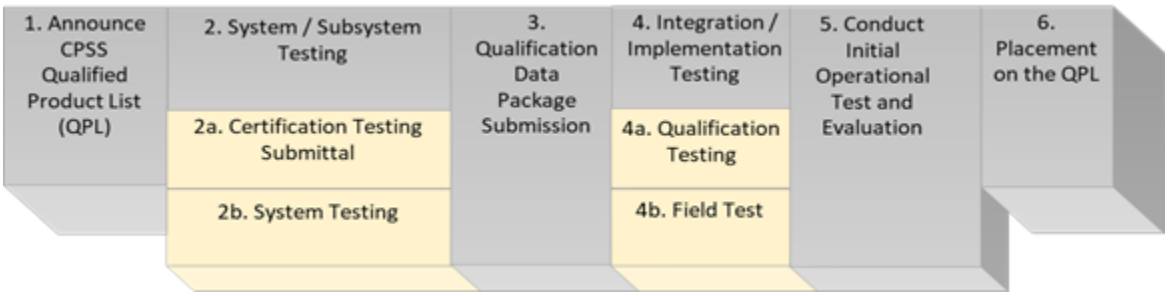

Figure 1. Qualification Process

1.2 Period of Performance

The CPSS QPL Overview will remain in effect until it is closed by TSA. TSA will open specific Windows of the QPL to notify QPL Applicants that they may submit their systems in response to this QPL. TSA anticipates conducting annual reviews to verify the need to open future QPL Windows to accommodate increasing capabilities in CT equipment over the life of the CPSS Program. Department of Homeland Security (DHS) Agencies/Components reserve the right to utilize the list of qualified vendors to issue their own contracts and orders.

1.3 Bailments

During the CPSS Qualification Process, the QPL Applicant will be required to provide the TSA with the proposed system via a bailment agreement. Terms and conditions of bailment agreements, including the time at which a bailment is needed, scope, and duration will be determined at each QPL Window and under official bailment agreements.

2.0 Qualification Process

The intention of the Qualification Process is to test and qualify systems to TSA standards, verify an executable manufacturing process, ensure operational supportability with particular attention to minimizing the logistics footprint, implement Human Systems Integration (HSI), ensure affordability, and demonstrate system integration, interoperability, safety, and utility.

QPL Applicant interested in having a system qualified under the CPSS Qualification Process must successfully meet both the requirements and the timeline for each step in the CPSS Qualification Process outlined in this overview, detailed in the QMP and provided within the specific notice for a given QPL Window. TSA anticipates issuing a notice to open a new QPL Window for each CPSS incremental enhancement, as discussed in paragraph 1.0 above.

Systems submitted under the CPSS QPL Windows are required to pass multiple levels of testing and receive approval by the TSA. Therefore, all CPSS systems proposed by the respective QPL Applicant to meet the identified requirements under the CPSS QPL will be required to pass all steps of the Qualification Process.

2.1 Step 1: Announce QPL

When TSA has a specific requirement, TSA will post a notice on FedBizOpps (FBO) opening a QPL Window for QPL Applicants to submit their systems and Qualification Data Packages (QDPs). A QPL Window is the time period when TSA will accept QPL submissions for entry into the Qualification Process

2.2 Step 2: System / Subsystem Testing

2.2.1 Decision Step 2a – Certification Testing Submittal

Certification (CERT) is the formal test that is administered to all candidate systems under the strictest controls possible. CERT consists of three parts: (1) the conventional explosives test, (2) the Home Made Explosives (HMEs) test, and (3) the false alarm test. The CERT team will utilize a standard test article set for the CERT of all CPSS systems. All test articles are scanned by the system as instructed by QPL Applicant operating manuals. During the conduct of CERT, the QPL Applicant may be called upon for technical and maintenance support, as required.

However, the QPL Applicant will not be permitted in the immediate test area unless requested by the DHS Transportation Security Laboratory (TSL) Test Director.

All systems seeking qualification under future CPSS QPL Windows will be required to undergo and pass CERT against the APSS detection standard. If an QPL Applicant's system fails the detection or false alarm requirement(s), the QPL Applicant must resubmit for CERT at a future time as coordinated with the TSL.

Upon successful completion of CERT, the TSA will provide the QPL Applicant a Certification Letter that identifies the system baseline and level of certification that is achieved. Also, the Government will add the system to a Certification Database that will identify both the system baseline that has been certified and the certification level achieved as a means to record compliance with 49 U.S.C. § 44913 explosives detection certification.

The systems shall have the same configurations with respect to components that could affect detection performance, including system hardware, software, and tuning parameters after the completion of CERT. No system modifications will be allowed after the completion of certification testing without the written approval from the Government.

2.2.2 Step 2b: System Testing

The QPL Applicant shall conduct internal system testing in accordance with the QPL Applicant System Test Plans and Procedures. The QPL Applicant shall procure or fabricate any special test articles and instrumentation for such tests. The QPL Applicant is responsible for contacting, communicating expectations, and acquiring results or reporting documentation for any third party testing utilized during the System Testing phase. The QPL Applicant must verify that any third party testers utilized are reputable and industry leaders in the field of verification. It is the QPL Applicant's responsibility to ensure the testing adequately verifies the requirement and that the data and documentation provided by the third party tester is thorough and complete.

During the execution of Step 2b: System / Subsystem Testing, the QPL Applicant shall identify all hardware and software defects and deficiencies found as a result of Step 2b: System / Subsystem Testing (internal QPL Applicant testing), and generate a Change Request package. The QPL Applicant shall submit all change packages to CPSSComms@tsa.dhs.gov in accordance with the APM Configuration Management Plan (Rev E) and Office Security Capabilities (OSC) Configuration Management Guidance Version 2; June 30, 2015.

2.3 Step 3: QDP Submission

The QPL Applicant shall generate a QDP for submission into the TSA Qualification Process, if accepted by TSA, the QPL Applicant system will continue into Step 4: Integration / Implementation Testing of the TSA Qualification Process.

In the QDP, the QPL Applicant shall provide all test data, evaluation tools (including simulations) and results to TSA for performance evaluation and to assist in the QDP acceptance decision. The QPL Applicant shall document any major issues experienced during QPL Applicant System Testing and document any system modifications which could impact previously completed, ongoing, or upcoming test events. TSA will review System Test results as part of reviewing and accepting the QDP.

The QPL Applicant's QDP must contain the required information and be presented in a manner that is clear, concise, and unambiguous, following the Data Item Description (DID). The QPL

Applicants must use proprietary and Sensitive Security Information (SSI) markings according to standard marking procedures. SSI must be handled according to the requirements of 49 Part 1520. The TSA Systems Integration Facility (TSIF) has instituted procedures to safeguard proprietary data that are used during CPSS QDP evaluation. The QDP will become a part of the official records of compliance testing for each system submitted.

The level of substantiation that needs to be submitted for each requirement is outlined in the CPSS FRD. Complete identification of the systems used to collect the substantiation data must be provided in the QDP and match the system being proposed for TSA testing. This includes:

a) Model number(s) of equipment tested.
b) Serial number(s) of equipment tested.
c) Software version(s), including reconstruction and inspection software components.
d) Firmware version(s), if applicable.
e) An inventory of hardware Configuration Items (CIs), software CIs, and firmware CIs with configuration identification as instructed through the Master Configuration Item List (MCIL) section.
f) Identification of all configurable and adjustable parameters and adaptation data used to tailor the system, as well as their settings and values. Adaptation data refers to variables used to configure or adjust the system to specific environments or uses. Unless required by the tests, all tests shall be conducted with the same parameter and adaptation settings. If changes to calibration settings or variable parameters are required, these must be clearly indicated along with an explanation for the changes.
g) Provide the United States equivalent if substantiation calls out European standards.

The QDP shall contain System Requirements, Architecture Documentation and Cybersecurity Documentation, a Life Cycle Support Concept, MCIL, cybersecurity information of the QPL Applicant development/test environment, and additional configuration management documentation, as detailed throughout this document. As a clarification, the cyber testing scope will assume an adversary with physical access to all CPSS systems (with varying access to system software). Though, cybersecurity information of the QPL Applicant development/test environment is requested, the TSA Test and Evaluation (T&E) scope will not consist of cyber testing in the QPL Applicant facility. The QDP shall also contain the Test Reports from QPL Applicant System / Subsystem Testing as verification of system readiness to proceed into independent Government T&E.

The QDP will be evaluated by the Government for thoroughness and adequacy to enter into independent Government T&E. Once approved, the QDP is the design basis in which the system baseline is established by the Physical Configuration Audit (PCA) for the remainder of the Qualification Process.

2.4 Step 4: Integration/Implementation Testing

The goal of Step 4 is to ensure the system meets requirements specified in the FRD, is ready to proceed into the Initial Operation Test and Evaluation (IOT&E), and will not pose any operational, safety, or security risks. During Step 4, the Government shall execute testing against requirements, assigned by the QT System Evaluator, as a verification test source. These are typically requirements from the FRD and IRD (if applicable). Testing for Step 4 will be

tailored to these requirements and all effort will be made to evaluate each System Under Test (SUT) in an identical manner. Step 4 will also include early user in the loop events.

The QPL Applicant shall deliver to TSA a proposed baseline system with all associated approved corrections following System / Subsystem Testing, for use in independent Government Integration/Implementation Testing (Qualification Testing (QT) and Field Test respectively). QT and Field Test will be performed independently from the QPL Applicant by the Government at the TSA TSIF and airport checkpoints in a true operational environment. QT will be focused on verification of requirements to include Critical Technical Parameters, Key Performance Parameters, Key System Attributes, Measures of Effectiveness, Measures of Suitability, Measures of Performance, and mission level performance in the controlled laboratory environment.

Integration or Implementation Testing will be tailored at the discretion of the TSA and may include early user in the loop events, system endurance tests integrated at an operational field site, Cybersecurity Vulnerability Scans, Networking Configuration validation, Privileged Access Management (PAM) credential validation, and an assessment of performance prior to the conduct of IOT&E.

2.4.1 Step 4a: Qualification Testing

QT is conducted by the TSA at the TSA TSIF to assess system performance against requirements in a laboratory environment and readiness for testing in the operational environment. The QPL Applicant shall provide the TSA with the proposed system for QT at the TSIF.

The QPL Applicant will not be permitted to witness QT. However, the QPL Applicant may be called upon for on-site technical support, cyber security verification activities (e.g., questions on security controls) and maintenance, or troubleshooting of system malfunctions, as required. With the exception of Field Data Reporting System (FDRS) and log files, the QPL Applicant shall not conduct data recording (logging) of test events or test objects. All image files, FDRS and log files generated during QT will be the property of the Government or will be purged from the system upon completion of the tests by the Government. The QPL Applicant will not be permitted to wipe any data from test equipment without the explicit approval of the Government employee, in writing, during a maintenance visit or at completion of QT.

2.4.1.1 QT Failures

The TSIF Test Branch will track and document all SUT failures, malfunctions, and / or anomalies encountered during QT. The TSIF Test Branch will review observed issues that affect testing activities and will coordinate with the QPL Applicant for resolution of any required corrective actions for critical failures.

QT will be suspended if the SUT malfunctions or has a critical failure that impedes the progress of testing, and cannot be repaired or replaced within three business days of QPL Applicant notification or a time frame specified by TSA. Repeated critical failures, or a critical failure that remains unresolved, may also result in suspension or termination of testing if the overall QT schedule is impacted. If it is determined at any time during QT that the SUT fails to meet requirements, testing may be suspended or terminated and the QPL Applicant will be notified by the Government.

TSA may perform re-test or regression testing following a repair or replacement of parts, or after any software modification.

The Government reserves the right to remove any QPL Applicant from QT and require third party substantiation of QPL Applicant fixes if:

- the SUT experiences at least one TSA defined significant failure during QT.
- TSA determines the TSE has an unacceptable cluster of non-significant failures during QT.
- TSA determines the TSE has significant issues prior to testing that will prevent passing QT or IOT&E.

2.4.1.2 QT Reporting

The TSIF Test Branch will produce a QT Report at the conclusion of test activities, after any deficiencies have been properly adjudicated. The QPL Applicant will be notified of test results after the conclusion of the QT reporting period. The next steps in the process will also be provided and may include termination, deficiency investigation, correction or continuation through the Qualification Process.

2.4.2 Step 4b: Field Test

Field Testing is conducted by the Government or Government's Authorized Agent in an operationally realistic environment prior to IOT&E and is used to ensure the SUT is installed, integrated and ready to proceed to IOT&E. This test event will be done in parallel, or immediately following QT, and used to inform IOT&E; it will serve as one last test prior to IOT&E to ensure a successful Operational Test outcome. Testing will be conducted at the operation field site identified by TSA, which will likely consist of the same sites where IOT&E will be conducted.

Field Testing objectives include but are not limited to:

1. Further system performance verification that can only be fully verified in the operationally representative environment;
2. Identify performance shortfalls and to ensure the highest chance of IOT&E success;
3. If necessary, completion of Hazards and Environmental Safety and Occupational Health trials in the operationally realistic environment to verify system safety analysis done during QT (Subset of Occupational Safety Health, and Environment testing from TSIF);
4. Initial assessment by TSA organizations of component SOPs and training to include:
    a. SOP evaluations to ensure the SOP is correct for IOT&E.
    b. Training verification to reduce the "learning curve" and ensure adherence to the SOP during IOT&E.
    c. Inform the Program Manager to determine if the SUT is ready to present to the Operational Test Agent (OTA) for IOT&E.

2.5 Step 5: Conduct Initial Operational Test and Evaluation

IOT&E is the final dedicated phase of the Qualification Process. It is the final evaluation of the system in a true operational environment. The IOT&E is conducted by the OTA independent of the QPL Applicant and CPSS Program Office. The QPL Applicant shall ensure the same system

configuration that successfully passed CERT and Qualification Testing is on all Field Test systems prior to the start of IOT&E.

IOT&E is conducted to:

- Determine system operational effectiveness, suitability, and cyber resilience.
- Identify operational deficiencies.
- Evaluate system capability against currently deployed capability to validate system utility.
- Provide information for developing and refining logistics support requirements for the system and training, SOP and Concept of Operations.
- Determine whether the technical publications and support equipment are adequate in the operational environment.

2.5.1 IOT&E Failures

In the event the proposed system does not pass testing or is suspended, the system will be removed from the Government test site(s). The QPL Applicant will be notified of the failure and the Government will provide Trouble Reports detailing the deficiencies observed. The QPL Applicant may be required to resolve the identified deficiencies and may be required to enter into Third Party Testing to verify the corrected deficiencies prior to re-entry into the TSA Qualification Process.

2.5.2 IOT&E Reporting

A System Evaluation Report (SER) will be generated by the OTA post IOT&E that will document operational effectiveness, suitability, and cyber resilience and will identify any deficiencies. The SER will be submitted to the TSA and DHS. The TSA will review the SER and may or may not provide the details to the QPL Applicant.

The QPL Applicant will be notified of test results after the conclusion of the IOT&E reporting period. The TSA will also advise the QPL Applicant of required next steps in the process, which may include termination and/or deficiency investigation/correction.

2.6 Decision Step 6 – Placement on QPL

Post IOT&E, a satisfactory finding of operational effectiveness, suitability, and cyber resilience, followed by a favorable DHS programmatic decision will result in that system being placed on the QPL. Once a system is added to the QPL it is considered “Qualified” and no additional qualification determination will be provided.

The TSA will provide test results and advise the QPL Applicant of the required next steps in the process.

3. Applicable Documents

All reference documents and guidance publications will be uploaded to this FBO notification and available to QPL Applicants. Reference documents that are Classified or contain SSI will not be uploaded to FBO, but may be requested at the opening of individual QPL Windows, per the guidance outlined in section 3.4 “Document Release Requirements”. Additional mandatory documentation and guidance publications may be provided at individual QPL Windows.

3.1 Reference Documents

The following documents form a basis for the certification and qualification of CPSS systems. These documents will be available to QPL Applicants on FBO:

a) CPSS Functional Requirements Document (FRD), Version 1.0
b) TSA APSS Detection Standard Version 6.2, Version 1.0, 05 October 2018
c) Security Technology Integrated Program (STIP) Enterprise Simulator Software Package
d) CPSS Certification Management Plan (CMP) (DHS/ST/TSL-19May 2019)
e) ASQC Q9001, Quality Systems-Model for Quality Assurance In-Depth, Development, Production, Installation, and Servicing
f) 49 USC, subsection 44913 – Explosives Detection

3.2 Guidance Publications

a) DHS Instruction 102-01 Acquisition Management Instruction
b) DHS Instruction 102-01-001 Acquisition Management Instruction Implementation
c) TSA Office Security Capabilities (OSC) Configuration Management Guidance Version 2
d) MIL-STD-31000A, Department of Defense Standard Practice Technical Data Packages, February 26, 2013TSA Test and Evaluation Policy, Revision 3
e) TSA/DHS Title 49 CFR Parts 15 and 1520, Transportation: Protection of Sensitive Security Information
f) TSA Management Directive 1400.3
g) TSA Information Assurance Handbook
h) NIST Special Publication (SP) 800-53
i) NIST Special Publication (SP) 800-37
j) Configuration Management Plan (CMP) for Acquisition Program Management, Revision E

3.3 Precedence

In the event of a conflict between the documents listed in 3.1 and 3.2, the documents in 3.1 shall take precedence. In the event of a conflict between the documents listed in 3.1, the QPL Applicant shall contact the Government and the Government will adjudicate on a case-by-case basis.

3.4 Document Release Requirements

To participate in the CPSS Qualification Process, QPL Applicants will need access to the below Classified, Sensitive Security Information (SSI), and Unclassified documents. QPL Applicants will be granted access to these documents <u>only at the opening of individual QPL Windows</u>.

- CPSS QMP – Unclassified
- CPSS Functional Requirements Document (FRD) - SSI

- STIP Enterprise Simulator Software Package – SSI
- APSS Detection Standard 6.2 – Classified

To access Classified documents, QPL Applicants must have a Facility Clearance Level (FCL), also known as an industrial security facility clearance. In addition, an administrative determination by the Defense Security Service (DSS) is necessary indicating that an QPL Applicant's facility is eligible for access to classified information of a certain category and all lower categories. Department of Defense (DD) Form DD 254 applies to the cleared facility.

To access SSI, QPL Applicants must obtain TSA authorization. The process to gain access to SSI is as follows:

1. Designate a Single Company Official (SCO) to oversee as the point of contact for the SSI. This individual must certify all appropriate protections will be followed, ensuring only authorized individuals will have access to the sensitive information, and those individuals adequately understand their responsibilities to protect the information.
2. Complete the Security Threat Assessment (STA) Request Form, following instructions therein, for all employees intending to handle SSI.
3. Provide signed non-disclosure agreements (NDAs) for all individuals listed in the STA Request Form.
4. The designated SCO must provide the Company's Data Protection Plan (DPP), which provides the procedures for:
    - Training employees who will receive SSI
    - Handling SSI
    - Transmitting SSI
    - Storing SSI
    - Destroying SSI when no longer needed by the organization

Upon SSI vetting completion, TSA will provide approval or denial to the QPL Applicant's SCO.

4.0 Applicable QPL Terms

In addition to the terms noted in this section, this QPL Overview for CPSS is governed by the policies and procedures set forth in FAR 9.2, Qualification Requirements. Additional QPL Terms may be included at individual QPL Windows.

4.1 TSA 5200.204.003 Requirements for Handling Classified National Security Information (Sep 2018)

A. **Clearance Level.** The CPSS Qualification Process requires a Secret security clearance.

B. **Access to Classified Information.** Contractor personnel are required to have access to classified information at the Secret level.

C. **Place of Performance.** The location of performance where classified information will be accessed, produced, safeguarded, or stored is as identified below:

[Determined at individual QPL Window]

If the Contractor supports other government agencies on classified contracts at the same facility, the TSA classified material shall be stored alone in a separate, GSA-approved safe. Classified information pertaining to other government agencies shall not be stored with the TSA classified information.

(End of Term)

4.2 TSA 5200.204.004 Requirements and Duties for Handling Sensitive Security Information (SSI) (SEP 2018)

Pursuant to 49 U.S.C. § 114(r), *Sensitive Security Information* and *Nondisclosure of Security Activities*, Sensitive Security Information (SSI) is a category of sensitive but unclassified (SBU) information that must be protected because it is information that, if publicly released, would be detrimental to the security of transportation. Under 49 Code of Federal Regulations Part 1520.5(a), the SSI Regulation also provides additional reasons for protecting information as SSI beyond the condition that the release of the information would be detrimental to the security of transportation. TSA, however, primarily uses the criterion of "detrimental to the security of transportation" when determining whether information is SSI.

The SSI regulations at 49 C.F.R., Part 1520 defines the scope, categorization, handling requirements and disposition of information deemed SSI (http://ecfr.gpoaccess.gov/). Persons authorized to access specific SSI (i.e., covered persons) include those contracted to DHS or TSA with a need-to-know basis for specific information in the course of fulfilling their TSA contractual obligations. TSA may deliver SSI materials to the Contractor. Also, materials created by the Contractor may require SSI designation and protection, and the Contractor has the responsibility to identify such materials to TSA as possible SSI. For guidance while working on TSA and DHS matters, see the TSA SSI Application Guide, 2011_04_01 for identifying the type of information covered by the regulation.

For purposes of this term, the term "Contractor" shall include an individual or other legal entity who performs work for or on behalf of TSA or DHS under a contract, interagency agreement, or other transaction agreement. Such contracts include, but are not limited to, contracts between any non-Federal entity and/or TSA or DHS and subcontracts, joint venture agreements, and teaming agreements between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the TSA or DHS.

While SSI is not classified national security information subject to the handling requirements governing classified information, it is subject to certain legal disclosure limitations. To ensure regulatory compliance, the Contractor shall be subject to the following requirements and include this entire term as flow-down in subcontracts, etc.:

A. **Handling and Safeguarding.** The TSA Contractor shall safeguard and handle any SSI in accordance with the policies and procedures outlined in 49 C.F.R. Part 1520, as well as the DHS and TSA policies and procedures for handling and safeguarding SSI. These safeguarding procedures shall include SSI recognition, identification and marking of materials that possibly contain SSI, including Contractor-created materials, as well as

following restrictions on disclosure, storage, handling, sharing, dissemination and destruction of SSI. The Contractor, without exception, shall place this requirement in all subcontracts, joint venture agreements, and teaming agreements related to the performance of this contract.

B. **Non-Disclosure Agreements (NDAs).** (DHS Form 11000-6, NDAs are required to be signed by all Contractor personnel when access to SSI is necessary for performance of the contract. By signing the NDA, the recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information.

C. **Request for Access to SSI materials.** Pursuant to 49 C.F.R. §1520.9(a)(3), the Contractor must contact SSI@tsa.dhs.gov for guidance on handling requests to access to SSI (before using SSI materials) for any other purpose besides activities falling within the scope of the contract by other persons, including requests from experts, consultants, and legal counsel ("requesters") hired by the Contractor. The Contractor shall include the Contracting Officer (CO) and Contracting Officer Representative (COR) as a carbon copy "cc" recipient of its contact to SSI@tsa.dhs.gov . The TSA SSI Office must first make a determination as to whether the requesters are a "covered person" with a "need to know" under 49 C.F.R. § 1520.7 and 1520.11. Special request processing and handling requirements apply to contractor employees who may be foreign nationals. The Contractor must clearly identify any employees who are not US citizens who are otherwise requested to have access to SSI; the requirements of TSA Management Directive 2810.3" "Management of Foreign Access to Sensitive Information" apply.

D. **Training and Certification.** All Contractor personnel who are covered persons with a need-to-know basis must complete the TSA-mandated SSI Awareness Training course prior to accessing SSI, and on an annual basis for the duration of the contract or for the duration of the requester's need for access to SSI, whichever is later. Contractor personnel must also review and adhere to the SSI Quick Reference Guide for DHS Employees and Contractors. The Contractor shall certify to the Contracting Officer annually that all covered persons have completed the mandated SSI training, that all SSI policies and procedures have been followed, and that those individuals with access understand their responsibilities to protect the information.

E. **Breach.** In accordance with 49 C.F.R. §1520.9(c), the Contractor agrees that in the event of any actual or suspected breach of SSI (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the Contractor shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer and the COR. The Contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government officials.

In the event that an SSI breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, or the Contractor's covered persons, the Contractor shall, as directed by the Contracting Officer and at no cost to the Government, without delay correct or mitigate the violation. For unauthorized disclosure of SSI, the Contractor and Contractor's

employees and Contractor's covered persons may also be subject to civil penalties and other consequences as set forth in 49 CFR § 1520.17.

(*End of Term*)

4.3 OFFEROR ACCESS TO SENSITIVE SECURITY INFORMATION (SSI) NECESSARY FOR PROPOSAL PREPARATION (JUL 2018)

QPL Applicants will be granted access to applicable SSI documents at the opening of individual QPL Windows per the guidance outlined in section 3.4 "Document Release Requirements".

A. Background. Sensitive Security Information (SSI) may be available to QPL Applicants in preparing responses to this acquisition. Potential QPL Applicants must obtain specific authorization in order to obtain SSI. SSI will not be available or otherwise provided or disclosed to any person not specifically authorized to receive it. SSI provided under this acquisition may only be used to satisfy acquisition requirements.

B. Senior Corporate Official. Each QPL Applicant (and subcontractor/team member) must separately designate in writing to the Contracting Officer a single, corporate official who will serve as the single point of contact for sensitive information. This individual must certify that all appropriate protections will be followed, only authorized individuals will have access to the sensitive information, and that those individuals adequately understand their responsibilities to protect the information. This official must also certify to the Contracting Officer every 60 days that all appropriate protections have been followed, only authorized individuals have access to the sensitive information, and that those individuals with access adequately understand their responsibilities to protect the information. A copy of this certification shall also be emailed to rfp.access@tsa.dhs.gov. This official will also ensure that the Contracting Officer is notified of staffing changes or circumstances in which individuals no longer need access to the information.

C. QPL Applicant Responsibility. TSA will review the System for Award Management (SAM) and Dunn and Bradstreet to ensure that the corporate entity would not otherwise be precluded from receiving a contract award. While this review does not replace the responsibility determination required by FAR part 9, it may prohibit QPL Applicants from receiving SSI information during the solicitation phase of the acquisition.

D. Criteria for Release. As part of this acquisition, SSI may only be accessed by individuals which 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 databases.

E. Information Requirements. Consistent with the criteria release described above, QPL Applicant's Senior Corporate Officials 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 whose access to the specified SSI and consequent input into the planned proposal is necessary to prepare and complete the proposal. All information must be emailed to rfp.access@tsa.dhs.gov. 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. Senior Corporate Officials shall provide the Contracting Officer via email with the CAGE code of the QPL Applicant's facility that will manage the proposal, company DUNS number, and address; and
2. Senior Corporate Officials shall provide the following information for all employees who require access to SSI in a single password protected Microsoft Excel spreadsheet emailed to the Contracting Officer. The password for the password protected spreadsheet shall be sent to the Contracting Officer in a separate email, at the same time.

   Employee Full Name

   Employee Gender: (i.e., Male or Female)

   Employee Birth Date:

   Employee Citizenship:

   Indication of whether any nominated employees have:

   Previously received a TSA suitability determination;

   Undergone a federal background investigation; or

   Possess an individual security clearance

   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. In those instances the Senior Corporate Official will receive an email from RFP.Access@tsa.dhs.gov requesting the Social Security Number for the select individuals and the Senior Corporate Official will provide the requested information back to RFP.Access@tsa.dhs.gov in a password protected document using the same password previously provided.

F. Privacy Act Statement. TSA will use the information provided to conduct a security threat assessment on individuals who seek access to Sensitive Security Information (SSI). The information 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 your security threat assessment, without which you may not be granted access to the SSI.

G. Notification of Assessment. Individuals who receive a successful Security Threat Assessment will be eligible to receive SSI. If it is determined that covered individuals are not eligible to receive access to particular SSI based on the threat assessment, TSA will provide the company point of contact notification that the individual does not qualify to receive SSI.

Appeal of the determination will not be permitted due to the time sensitive nature of the acquisition process, however, the potential offeror may nominate another individual to receive SSI access. In the event that an individual is determined to be a security threat and the individual believes that the results of the screening 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 However, due to the demanding acquisition schedule, TSA will not delay an acquisition to resolve these issues.

H. Non-Disclosure Agreements. Each QPL Applicant employee 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 with and as part of the submission of information reflected in Paragraph E above. The QPL Applicant should understand that employees 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 in the pre-award phase does not substitute such requirement post award.

I. Return of SSI. Any SSI provided for purposes of the subject Qualified Product List (QPL) application must be returned to the Government and verified by the Government. For solicitations where an offeror submits a proposal, the SSI shall be returned prior to the beginning of proposal evaluations. If the vendor elects not to submit a proposal, any SSI shall be returned by the closing date of the solicitation. For QPL applicants, any SSI shall be returned upon notification of either acceptance or rejection to the QPL.

(End of Term)

4.4 TSA 5200.224.002 Controlled Unclassified Information Data Privacy and Protection (DEC 2015)

The Contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the Government ii) Government data transmitted by the contractor, and iii) Government data otherwise stored or processed by the contractor, regardless of who owns or controls the underlying systems while that data is under the contractor's control.

All Government data, including but not limited to Personal Identifiable Information (PII), Sensitive Security Information (SSI), and Sensitive but Unclassified (SBU), and/or Critical Infrastructure Information (CII), shall be protected according to Department of Homeland Security information security policies and mandates.

At the expiration of the contract, the contractor shall return all Government information and IT resources provided to the contractor during the contract.

The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow all applicable DHS Component Agency's requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI, Informational Security and Privacy training, if required by the DHS Component Agency.

The Contractor, and those operating on its behalf, shall adhere to the requirements of the non-disclosure agreement unless authorized in writing by the Contracting Officer.

The Government will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment as applicable. If encryption is required, the following methods are acceptable for encrypting sensitive information:

A. Products Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2.

B. National Security Agency (NSA) Type 2 or Type 1 encryption.

C. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

The contractor shall maintain data control according to the applicable DHS Component Agency's security level of the data. Data separation will include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII must comply with TSA MD 3700.4 if applicable.

Users of Government IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing Government IT assets are expected to actively apply the practices specified in the TSA Information Technology Security Policy (ITSP) Handbook, Chapter 3, Section 6, Privacy and Acceptable Use, or similar DHS Component Agency's guidance or policy.

The contractor shall comply with the all data disposition requirements stated in the applicable DHS Component Agency's Information Security Policy. For all TSA orders the contractor shall comply with Information Security Policy Handbook Chapter 3, Section 17 Computer Data Storage Disposition, as well as TSA Management Directive 3700.4.

(End of Term)

4.5 TSA 5200.209.005 Notification to Offerors of Contractor Support of the Selection Process (Jul 2018)

A. Offerors are advised that employees of the firms identified below may serve as Source Selection Organization members or provide other support in the source selection process. These individuals will be authorized access to only those portions of proposal data and discussions that are necessary to enable them to perform their respective duties. Such firms are expressly prohibited from competing on the subject acquisition, from rating of proposals or recommending the selection of a source, and from revealing who the competing firms are to anyone without a valid need-to-know.

(The Contracting Officer should enter the firms' names here): If applicable, below information will be provided for each QPL Window.

- Firm #1
- Firm #2
- Firm #3, etc.

Legal Business Name(s) of Firm(s): _____

Current Address of Firm (Official Street, City, State, Zip Code and Telephone #):

_____

_____

B. In accomplishing their duties related to the source selection process, the aforementioned firms may require access to proprietary information contained in the offerors proposals. Therefore, pursuant to FAR 9.505-4, these firms must execute an agreement with each Offeror that states that they will: (1) protect the offerors 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 evaluation process, each Offeror must contact the above companies to effect execution of such an agreement prior to submission of proposals. Each Offeror shall submit copies of the agreement with their proposal.

(End of Term)

5.0 Contact Information

RFP.Access@tsa.dhs.gov email is to be used for SSI requests only. All other communications regarding this notice, shall be sent via e-mail to CPSSComms@tsa.dhs.gov. It is the QPL Applicant's responsibility to ensure email receipt is confirmed.

The TSA will not accept any submissions as a result of this QPL Overview notice; all submissions will be accepted at individual QPL Windows. Similarly, request for SSI, Questions and Answers (Q&A), and all other requests/submissions will be limited to the period specified in the QPL Window.

This notice is for information purposes only and shall not be construed as a commitment or a promise of a contract by the Government. The Government will not pay any costs incurred in the submission of responses to this notice. The QPL Applicant is responsible for all costs associated with their participation in and submission to this QPL.