Privacy Impact Assessment Update
for the

Access to Sensitive Security Information (SSI) in Contract Solicitations

DHS/TSA/PIA-030(b)

February 19, 2019

Contact Point
Marvin Grubbs
Contracting & Procurement
Transportation Security Administration
TSAProcurementPolicy@tsa.dhs.gov

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) conducts security threat assessments on individuals and companies that seek access to Sensitive Security Information (SSI) necessary to prepare a proposal in the pre-award phase of contracting with TSA. SSI is a form of unclassified information that, if publicly released, would be detrimental to transportation security.[1] Pursuant to the Aviation and Transportation Security Act (ATSA),[2] TSA also enters Other Transaction Agreements (OTA), procurement contracts, and other agreements with various public and private entities in furtherance of its security mission, and receives submissions for the Qualified Products List (QPL). In certain cases, TSA may need to conduct security threat assessments (STA) on individuals and entities that seek access to SSI necessary to prepare a proposal or submission in response to these situations. TSA is updating this Privacy Impact Assessment (PIA) to address the collection of Personally Identifiable Information (PII) from members of the public before granting access to SSI and to clarify the records retention.

Introduction

TSA primarily awards procurement contracts through a full and open competitive process governed by the Competition in Contracting Act[3] and the Federal Acquisition Regulation (FAR). This process, in which industry is publicly invited to submit proposals, requires that sufficient information is uniformly provided to industry such that competitive proposals may be developed in a fair marketplace. If determined necessary by TSA, some vendors may require access to SSI in the form of program-specific technical specifications, test results on vendor technology, testing processes, or responses to vendor questions. The solicitation notice will indicate whether SSI access is required. Timely release of program-specific SSI information will prevent delays in the projected contract award and ultimately enable enhanced operations.

In addition to procurement contracts, TSA also awards and administers OTAs in furtherance of the agency's mission. While an OTA is not a procurement contract, it may involve the issuance of a solicitation. Depending on requirements, some OTAs may involve SSI, such as airport security operations or technical specifications, and thus may require an entity's access to SSI in order to submit a proposal. In addition to OTAs, TSA enters into other agreements with various public and private entities in support and furtherance of its security mission. Some of these agreements may require access to SSI prior to their execution. TSA also receives proposals for QPLs, some of which may require access to SSI prior to submission.

TSA collects PII from members of the public before granting access to the minimum SSI required for purposes of preparing proposals and other submissions. PII collected through this

[1] 49 CFR Part 1520.
[2] 49 U.S.C. § 114.
[3] 41 U.S.C. § 253.

process is maintained in accordance with the Privacy Act of 1974 and TSA's System of Record Notice (SORN) DHS/TSA-002 Transportation Security Threat Assessment System (T-STAS).[4] TSA is updating this PIA to expand the population from which PII is collected and to update the records retention process. The information provided in the previously published PIAs from September 2010, and July 2012, remains in effect.

Reason for the PIA Update

TSA is updating this PIA to expand the population of offerors subject to the STA requirement to include individuals who respond not only to procurement contract solicitations, but other types of transactions including OTAs, other agreements, or QPLs. This PIA also reflects the revised records retention process for the PII collected. With this update, Contracting & Procurement (C&P) will no longer maintain the PII collected for the purpose of conducting STAs in official contract files.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There are no changes to the type of information collected by this activity. This update expands the population of offerors from which PII is collected to include those responding to solicitations for OTAs, other agreements, or QPLs. The previous PIAs only addressed the collection of PII from individuals and entities responding to TSA procurement contract solicitations.

Uses of the System and the Information

No change.

Retention

Like DHS, TSA follows the retention schedules for procurement solicitations, offerors and procurement contracts published in the FAR.[5] Until recently, C&P maintained all PII collected for the purpose of conducting STAs in the official contract file; however, the FAR requires that contract files include "the list of sources solicited, and a list of any firms or persons whose requests for copies of the solicitation were denied, together with the reasons for the denial."[6] C&P can accomplish this requirement without retaining all PII collected; thus, contract files will no longer retain all PII necessary to conduct an STA, such as Social Security number or fingerprints. This revision will help to eliminate the maintenance of duplicative PII and will result in a shorter

[4] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (August 11, 2014).
[5] 48 CFR Part 4.802.
[6] 48 CFR Part 4.803.

retention schedule for most of the PII collected. (For purposes of consistency, the same schedule and process apply to OTAs and other agreements awarded by C&P.)

PII maintained by C&P will be securely stored until the final proposal due date; issuance of an affected QPL acceptance or denial letter; or until issuance of the agreement. C&P will not maintain copies of STAs. PII collected for the purpose of an STA and the STA results are securely maintained in TSA's Transportation Vetting System and no longer in the official contract file.[7] The NARA-approved records schedule for information collected for the purpose of conducting STAs is as follows:

- For individuals who were not near matches to a government watchlist, records will be destroyed one year after the access privilege is no longer valid (DAA-0563-2013-0001-0008);[8]
- For individuals that were near matches to a government watchlist and subsequently cleared, records will be maintained for seven years after the access privilege is no longer valid (DAA-0563-2013-0001-0009);
- When the individual is an actual match to a watchlist, records will be destroyed 99 years after the STA or seven years after TSA is notified that the individual is deceased, whichever is shorter (DAA-0563-2013-0001-0010).

Internal Sharing and Disclosure

No changes.

External Sharing and Disclosure

No changes.

Notice

No changes.

Individual Access, Redress, and Correction

No changes.

Technical Access and Security

No changes.

[7] *See* DHS/TSA/PIA-042 TSA Intelligence & Analysis' Technology Infrastructure Modernization (TIM) Program (March 26, 2014), *available at* https://www.dhs.gov/privacy.

[8] DAA-0563-2013-0001-0008, DAA-0563-2013-0001-0009 and DAA-0563-2013-0001-0010 Retention Schedules *available at* https://www.archives.gov/.

Technology

No changes.

Responsible Officials

Marvin Grubbs
Director, Competition Advocate and Task/Delivery Order Ombudsman
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security