Privacy Impact Assessment
for
Access to Sensitive Security Information in Contract Solicitations

September 9, 2010

Contact Point

Ronald Gallihugh
Office of Acquisition
Transportation Security Administration
TSAProcurementPolicy@dhs.gov

Reviewing Official

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Transportation Security Administration (TSA) is responsible for the acquisition of services and supplies related to protecting the nation's transportation system. If determined necessary for the proposal preparation process, TSA may permit offerors to have access to Sensitive Security Information (SSI) necessary to prepare a proposal. SSI is a form of unclassified information that if publicly released would be detrimental to transportation security. The standards governing SSI are promulgated under 49 U.S.C. §114(r) in 49 C.F.R. part 1520. In order to determine if a potential offeror may be granted access to SSI in the pre-contract award acquisition process, TSA will conduct a security threat assessment (STA) of the individuals and company. The STA 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. Because this program entails a new collection of information about members of the public in identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Overview

TSA primarily awards contracts through a full and open competitive process governed by the Competition in Contracting Act and the Federal Acquisition Regulation. This process, in which industry is publically invited to submit proposals, requires that sufficient information is uniformly provided to the industry, such that competitive proposals may be developed in a fair marketplace. If determined necessary by TSA, some contracts 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, which may contain SSI. 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.

TSA will use Personally Identifiable Information (PII) to assess individuals, before granting individuals and their company access to the limited SSI required for purposes of preparing contract offers. The designated company official will certify that the individual requires access to the SSI, and that the individual consents to submitting PII to TSA. TSA will exercise its discretion in assessing whether a company or individual will be entitled to receive SSI.

Section 1.0
Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

TSA may collect the full name (including any aliases), date of birth, place of birth, gender, Social Security Number (voluntary), fingerprints, and employer name and address of those individuals seeking access to SSI for use in responding to TSA contract solicitations. TSA will also retain the results of the

checks performed by TSA, as individuals who have already been through a redress process may wish to submit their redress number to avoid misidentification. In the event that an individual seeks redress, additional PII will be collected in order to communicate with the individual (address, phone, email address) and to determine whether the individual is a match to an individual listed in the database. The individual may be asked to submit supporting documentation, such as a copy of his or her passport or copies of at least three of the following: a birth certificate, driver's license, immigrant/nonimmigrant visa, naturalization certificate, certificate of citizenship, voter registration card, certificate of release or discharge from active duty, government identification card or military identification card. If the individual submits a birth certificate, it must be a certified copy of the original. TSA will also collect and maintain in official contract files a certification from each company that its employees that have access to SSI are properly trained, and TSA will also collect and maintain Non-Disclosure Agreements for each individual with access to SSI.

1.2 What are the sources of the information in the system?

TSA will collect PII from individual employees or their company representative, who are potential offerors on TSA contract solicitations that require access to SSI. Access may only be granted to a limited number of persons per company, as designated by TSA. TSA will also obtain information in the course of performing checks, such as government databases and commercially available sources, such as Dunn & Bradstreet.

1.3 Why is the information being collected, used, disseminated or maintained?

Information is being collected to perform a STA before granting access to particular SSI for use in responding to contract solicitations.

1.4 How is the information collected?

Companies interested in responding to contract solicitations will provide the SSI point of contact in the TSA Office of Acquisition with a password protected spreadsheet that contains the required information on individual employees via email. In the event of biometric information, individuals will either mail fingerprints to the TSA Office of Personnel Security or use TSA facilities to take the fingerprints.

1.5 How will the information be checked for accuracy?

The information will be obtained directly from the individual or representative of the company. TSA expects that individuals will submit accurate information. A senior corporate official from the potential offeror will be required to provide a certification attesting to the accuracy of the information. If a negative determination is made, individuals will have an opportunity for redress.

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

TSA has broad authority to carry out transportation security responsibilities under 49 U.S.C. §114(f), including assessing threats to transportation security. It also authorizes TSA to develop policies, strategies, and plans for dealing with threats to transportation security. SSI authority comes from 49 U.S.C. §114(r), with regulations promulgated in 49 C.F.R. Part 1520.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The incorrect identification of an individual as a security threat (false positives) is one of the privacy risks associated with this collection. TSA seeks to reduce the potential for misidentification by requesting sufficient information in order to distinguish the individual from others that may have the same name. TSA's privacy challenge is to mitigate the risk of false positives while ensuring that access to SSI is appropriately granted. It is critical that false positives be kept to a minimum, since they could result in the delay or denial of access to SSI that may affect timely acquisition of services and supplies that directly support transportation security efforts.

Section 2.0
Uses of the information

2.1 Describe all the uses of information.

TSA will use the information to conduct STAs, which will include a name-based check against Federal law enforcement, terrorism, and immigration databases and/or a Criminal History Record Check (CHRC. The results of the STA will be used by TSA to make a final determination on whether the individual may be granted access to SSI.

2.2 What types of tools are used to analyze data and what type of data may be produced?

None.

2.3 If the system uses commercial or publicly available data please explain why and how it is used?

TSA will use public information, or commercially available databases, such as Dunn & Bradstreet, to determine if a company or its officers represents a security threat. For example, TSA may use publically available information for materials reflecting a legitimate business presence sufficient to conclude that the company likely does not pose a security risk and is a legitimate entity.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The privacy risks associated with this collection involve insecure data transmission and inappropriate access. To mitigate the data security risk, company officials will be instructed to securely transmit data to TSA. To mitigate the opportunity for inappropriate access, TSA will share it only with those individuals who have a need to know the information in the performance of their official duties. In addition, it is expected that the number of individuals requiring a risk evaluation for access to SSI is very small and unlikely to be inappropriately accessed.

Section 3.0
Retention

3.1 What information is retained?

The information identified in section 1.1 will be retained.

3.2 How long is the information retained?

In accordance with the TSA Records Schedule and the requirements of the FAR, information identifying the results of the STA will be maintained in the official contract file and preserved for six (6) years and three months following the close-out of the contract.

3.3 Has the retention schedule been approved by the component records officer and National Archives and Records Administration (NARA)?

Yes.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Information collected through this program will be maintained in accordance with NARA approved schedules, in furtherance of TSA's mission to ensure the security of the Nation's transportation system. The retention period is designed to permit records to be retained in accordance with FAR requirements.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

In the ordinary course, it is expected that information will be shared with TSA employees or contractors in the Office of Transportation Threat Assessment and Credentialing, the SSI Branch, the Office of Personnel Security, the Office of Acquisition, Office of Information Technology/Chief Information Officer, Office of Chief Counsel, the Office of Intelligence, as well as the office responsible for the acquisition in order to conduct the STA and assess or act on the results, including providing SSI to approved individuals. Information might also be shared with the Office of Civil Rights and Civil Liberties, Privacy Office, Ombudsman, and Legislative Affairs to respond to complaints from individuals or perform functions assigned to those offices. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. While it is not expected that information will be routinely shared outside of TSA, TSA may need to share information with DHS employees who have a need to know in the performance of official duties. Any information shared within DHS will be retained in accordance with the applicable SORNs.

4.2 How is the information transmitted or disclosed?

TSA will transmit this data within DHS electronically, via password-protected email, or telephonically to those who need the information to perform their official duties.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information is shared within DHS with those individuals who have a need for the information to perform their official duties in accordance with the Privacy Act. Only DHS employees and contractors with proper access privileges are allowed access to this information to conduct risk evaluations. Employees authorized to access the data receive appropriate privacy and security training and have necessary background investigations and security clearances for access to sensitive or classified information. Privacy protections include strict access controls, security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared, what information is shared, and for what purpose?

TSA expects to share the results of the STA with the submitting official for purposes of notifying the company whether the individual may access SSI for purposes of preparing the offer. In the ordinary course of business, TSA does not expect to otherwise share collected information outside of DHS. Information will be shared with the Terrorist Screening Center and other agencies in connection with the resolution of possible name matches and any operational response. Further, TSA may share the information it receives with Federal, State, local, or tribal law enforcement or intelligence agencies 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 May 19, 2010 and can be found at 75 FR 28046-28051

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. TSA may share the information it receives with Federal, State, local, or tribal law enforcement or intelligence agencies 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 May 19, 2010, and can be found at 75 FR 28046-28051.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information may be disclosed in person, telephonically, electronically, by mail, password protected files sent by email, facsimile, or on a password-protected CD.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy risks associated with external sharing include sharing the results of the check with the employer of the individual which may result in adverse consequences to the individual. The risk is

mitigated by providing the individual with redress as described below. Other external sharing risks are mitigated by limiting external sharing in accordance with the Privacy Act and published SORN.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes. TSA will include a Privacy Act Statement in all contract solicitations and other pre-award acquisition actions where SSI may be provided to potential offerors so that individuals who seek access to SSI may exercise informed consent before providing personal information for the security threat assessment.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. The information is only required if the individual has been chosen as a representative by their employer to receive SSI. Individuals who do not wish to provide information should inform their employer and may decline to provide the information. However, if this information is not provided, TSA will not be able to complete a STA, without which the individual may not be granted access to the SSI. If additional information is needed during the redress process, that collection will also be voluntary and dependent upon the individual's desire to engage the redress process.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. However, all uses of such information by TSA will be consistent with the Privacy Act.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

TSA has made the process for transmission of individual information to TSA transparent. TSA will incorporate a Privacy Act statement in the contract solicitation, which will explain the authority for the collection, the purpose of the collection, the voluntary nature of providing the information, and that failure to provide the information may not permit TSA to complete a STA, without which the individual may not be granted access to the SSI. By providing this statement, individuals are given meaningful

notice that enables them to exercise informed consent prior to disclosing any information to TSA. Individuals will be aware of the collection.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20
FOIA Division
601 South 12th Street
Arlington, VA 20598-6020

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If it is determined that an individual is not eligible to receive access to particular SSI based on the STA, TSA will provide the individual and company point of contact a written determination that the individual does not qualify to receive SSI, and describe the process by which the individual may pursue redress. Due to the demanding acquisition schedule, however, TSA will not delay an acquisition to resolve any redress request. As warranted, the potential offeror may nominate another individual to receive SSI access. If an individual is disqualified because of the CHRC, the individual must notify TSA in writing of his or her intent to correct any information believed to be inaccurate within 30 days of being advised of disqualifying information. The individual is responsible for correcting information by contacting the law enforcement jurisdiction responsible for the information and providing TSA with a copy of the corrected record.

If the applicant believes he or she has been wrongly identified as a security threat, TSA provides a redress process and information on how to obtain releasable materials regarding this threat identification. There may be information or materials that are classified or otherwise protected by law or regulation that TSA cannot disclose.

7.3 How are individuals notified of the procedures for correcting their information?

TSA will provide a written determination that includes instructions for correcting information to the individual and the company point of contact.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A. A redress process, as described in section 7.2 above, is provided for individuals who believe that they have been incorrectly identified as a threat.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how the risks are mitigated.

There is little privacy risk associated with redress. Redress is the process by which an individual can correct inaccurate information unearthed during the threat assessment. TSA maintains all information collected during the threat assessment and redress process in accordance with the Privacy Act.

Section 8.0
Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Unauthorized access is avoided through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards that are in place. All government and contract personnel who require access to perform their official duties have passed personnel, physical, and network verifications.

All government and contractor personnel are vetted and approved for access to the facility where the system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides overall guidance on how employees are to protect their physical and technical environment and the data accessed to perform their official duties. All new employees are required to read and sign a copy of the TSA Rules of Behavior prior to getting access to any TSA IT system.

8.2 Will Department contractors have access to the system?

Yes. Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Adherence to access control policies is enforced by the system in coordination with and through oversight. All contractors performing this work are subjected to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All government and contractor personnel are required to complete TSA Privacy Training. Compliance with this requirement is audited by the TSA Privacy Officer. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Information in TSA's record systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. All systems are operating on the authority of the Designated Accrediting Authority (DAA). The Screening Gateway system completed FISMA Certification and Accreditation on December 30, 2009

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system maintains a real-time auditing function on individuals who access the system. Weekly logs are reviewed to ensure no unauthorized access has taken place. All TSA IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks include unauthorized access. Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and

integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access.

Section 9.0
Technology

9.1 What type of project is the program or system?

The program involves matching of limited PII to Federal contractor and security clearance databases, and in some cases will involve matching against terrorism watchlists or law enforcement databases.

9.2 What stage of development is the system in and what project development lifecycle was used?

The program is operational. No development lifecycle was used.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Official

Ronald Gallihugh

Office of Acquisition

Transportation Security Administration

Arlington, VA 20598

Approval Signature Page

(Original signed copy on file with the DHS Privacy Office)

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security