Privacy Impact Assessment
for the

Port Authority of New York/New Jersey Secure Worker Access Consortium Vetting Services

DHS/TSA/PIA-040

November 14, 2012

Contact Point
Joseph Salvator
Transportation Security Administration
Office of Intelligence & Analysis
Joseph.Salvator@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) will conduct terrorism watch list checks of workers at Port Authority of New York/New Jersey (PANYNJ) facilities and job sites, including critical infrastructure such as airports, marine ports, bus terminals, rail transit facilities, bridges, tunnels, and real estate such as the World Trade Center memorial site. TSA will also conduct terrorism watch list checks of individuals identified by PANYNJ as requiring such checks for access to sensitive information, and for workers at facilities and job sites of PANYNJ regional partners. Results of the checks will not be reported to PANYNJ, but instead will be forwarded to the Federal Bureau of Investigation (FBI) Terrorist Screening Center (TSC). This Privacy Impact Assessment (PIA) is conducted pursuant to the E-Government Act of 2002 because personally identifiable information (PII) will be collected for the conduct of terrorism watch list checks of workers at PANYNJ facilities and job sites.

Overview

Pursuant to 49 U.S.C. § 114, the Transportation Security Administration (TSA) is responsible for security in all modes of transportation. Currently, the Port Authority of New York/New Jersey (PANYNJ) Secure Worker Access Consortium (SWAC), a security access clearance/control program, conducts identity verification and criminal/immigration background checks for the credentialing of all personnel who have a need to access confidential information or restricted critical infrastructure security areas under the direct control of the PANYNJ. Such infrastructure includes airports, marine ports, bus terminals, rail transit facilities, bridges, tunnels, and real estate such as the World Trade Center memorial site which fall under the control of PANYNJ. TSA will also conduct terrorism watch list checks of individuals identified by PANYNJ as requiring such checks for access to sensitive information, and for workers at facilities and job sites of PANYNJ regional partners. Regional partners include such agencies as New Jersey Transit, New Jersey Turnpike Authority, and New York State Thruway Authority. Homeland Security Presidential Directive-6 (HSPD-6), *Integration and Use of Screening Information*,[1] states that it is the policy of the United States to develop, integrate, and maintain current terrorist information, and to use that information as appropriate and to the full extent permitted by law to support federal, state, local, territorial, tribal, foreign-government, and private-sector screening processes.

To support a private-sector screening process with a substantial bearing on homeland security, TSA has agreed to a PANYNJ request that TSA conduct checks of the foregoing individuals against the Terrorist Screening Database (TSDB) maintained by the TSC. PANYNJ will provide Personally Identifiable Information (PII) already collected for its own SWAC security checks to the TSA for recurrent vetting against the TSDB. PANYNJ currently provides affected individuals with notice that it will conduct a background check that encompasses a check of terrorism, criminal, and immigration databases. PANYNJ will provide notice to affected individuals that their PII will be provided to TSA. PANYNJ requires each affected individual to affirm that the information submitted to the PANYNJ SWAC program for this purpose is true, correct, and complete. TSA will forward all positive and

[1] http://www.fas.org/irp/offdocs/nspd/hspd-6.html

potential matches to the TSC, which will make final match determinations and coordinate any necessary response.

As part of this process, TSA may request additional information about an individual in order to clarify data errors or to resolve potential matches (e.g., in situations where an affected individual has a common name). Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB. Upon final determination by the TSC that an individual is a positive match, TSA and federal law enforcement agencies will be notified as appropriate. TSA will not provide vetting results to PANYNJ, nor will it provide results to an affected individual whose information has been submitted by PANYNJ.

PANYNJ will notify TSA when the individual is no longer part of the population for which a TSDB check is required. The recurrent vetting on these individuals are conducted and stored by TSA's Transportation Vetting System.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71; Nov. 19, 2002 (49 U.S.C. § 114). 49 U.S.C. § 114(f) grants authority to, among other things, assess threats to transportation, serve as the primary liaison for transportation security to the intelligence and law enforcement communities, and carry out such other duties relating to transportation security as the TSA Administrator considers appropriate. 49 U.S.C. § 114(m)(1) grants the TSA Administrator all authority conferred under 49 U.S.C. § 106(l)(6), and, together with 6 U.S.C. § 469, authorizes TSA to enter into agreements for security threat assessments and attendant fee collections on such terms and conditions as the TSA Administrator considers appropriate. Homeland Security Presidential Directive-6 (HSPD-6), *Integration and Use of Screening Information* directs the heads of executive departments and agencies to protect the United States against terrorism by, among other things, supporting private-sector screening processes.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS/TSA-002 Transportation Security Threat Assessment System of Records (TSTAS), 75 FR 28046 (May 19, 2010).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. Authority to Operate was granted on 31 August 2011.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. See section 5.0 below.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This initiative is not covered by the Paperwork Reduction Act. TSA is not conducting or sponsoring the collection (which is conducted by PANYNJ SWAC as part of its independent requirements).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The PANYNJ SWAC program collects PII from workers at PANYNJ and regional partner facilities and job sites as part of its existing security clearance process, as well as individuals PANYNJ requires to undergo checks for access to sensitive information, and will provide, if available or applicable, the following to TSA:

- Full name;
- Date of birth;
- Gender;
- Social Security Number;
- Citizenship;
- Passport Number with Country of Issuance, and/or Alien Registration Number; and
- known aliases and/or place of birth (optional).

TSA may request additional information about affected individuals submitted by the PANYNJ SWAC Program in order to clarify data errors or to resolve potential matches (e.g., in situations where an affected individual has a common name).

TSA will compare individual PII against the TSDB and will retain the match results.

2.2 What are the sources of the information and how is the information collected for the project?

PANYNJ will provide worker PII to TSA that it has collected for its own security checks. TSA will access the data through a secure website hosted by PANYNJ.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. TSA does not use commercial data or publicly available data in order to accomplish the TSDB check.

2.4 Discuss how accuracy of the data is ensured.

TSA relies on the accuracy of the information provided to it by PANYNJ. PANYNJ uses the same information for existing security checks that it performs on its workers. Workers must certify that the information provided is accurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that incorrect identification of an affected individual as a match to the TSDB may occur due to the submission of inaccurate or limited PII to TSA by PANYNJ.

Mitigation: TSA seeks to reduce the potential for misidentification by: (1) requiring data elements that should be sufficient to distinguish each affected individual from individuals whose information is included in the TSDB; and (2) collecting, as optional data, information that can reduce even further the potential for misidentification (e.g., both citizenship and gender may be provided rather than just one data point or the other). TSA will further mitigate the risk of misidentification by requiring PANYNJ to certify the accuracy, to the best of its knowledge, of the PII submitted to TSA.

Privacy Risk: There is a risk that adverse action may be taken against an individual from erroneous information**.**

Mitigation: The privacy risk is mitigated by collecting information that has already been used by PANYNJ to conduct security checks on its workforce, and the information is pulled directly from a secure website hosted by PANYNJ reducing transcription errors. The information is certified by the individual as being accurate. The risk is further mitigated because TSA performs only the limited function of identifying potential matches to the TSDB, which are then forwarded to TSC for confirmation and any operational response. TSA does not notify PANYNJ of the result, nor does it direct that PANYNJ or TSC take any action based on the result of the match.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

TSA will use the collected PII to recurrently vet against the TSDB for terrorism checks. If the individual is determined to be a match or potential match, that information will be forwarded to the FBI's TSC for review, use, and further dissemination as appropriate. TSA may use match information to facilitate operational, law enforcement, or intelligence-related responses by TSC.

TSA may use collected information to verify that an individual has been or is currently enrolled in a DHS program, such as the Transportation Worker Identification Credential (TWIC) Program or Hazardous Materials Endorsement (HME), which includes a TSDB check equivalent to the TSDB vetting performed as part of the PANYNJ Security Program.

TSA may conduct audits and data accuracy reviews as part of the PANYNJ Security Program. To assist with this activity, TSA may randomly request information previously provided to TSA from the PANYNJ SWAC Program on a small percentage of affected individuals to confirm its accuracy.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII may be used inappropriately.

Mitigation: The population covered by this program represents a small fraction of the individuals for whom TSA performs security threat assessments; therefore, the risk that the information for this population will be used inappropriately is extremely small. PII collected by TSA will be used only in accordance with the described uses by integrating administrative, technical, and physical security controls that place limitations on the collection of PII, and protect PII against unauthorized disclosure, use, modification, or destruction. The information will be used to identify potential matches to the TSDB, which will be confirmed by the TSC.

Privacy Risk: There is a risk that adverse action may be taken against an individual from requesting additional information.

Mitigation: TSA will not report any positive, potential, inconclusive, or negative matches to PANYNJ, and will not reveal to PANYNJ the names or any other identifying information of the individuals who are positive, potential, inconclusive, or negative matches.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

PANYNJ has already provided notice to its workforce that PII is being collected for purposes of security checks, including law enforcement, terrorism, and immigration checks. PANYNJ will provide additional notice in its SWAC application form and by letter to pre-existing workers that PII is being submitted to TSA for purposes of terrorism checks. Notice is also provided by the publication of this PIA.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

TSA does not regulate the relationship between PANYNJ and its workforce, and cannot comment on what opportunities there are for individuals to consent to uses, decline to provide information, or opt out. Individuals who do not provide information to PANYNJ for purposes of providing the information to TSA will not receive a TSDB check by TSA.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not know their information is provided to TSA.

Mitigation: The risk is mitigated by the fact that the PANYNJ will provide notice to the individual that their PII will be provided to TSA, the information collection by PANYNJ is overt, and the cooperation of the individual is required during their PANYNJ SWAC submission process.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The length of time TSA will retain biographic information and TSDB check results on an individual is based on each individuals' vetting result. Information will be retained as described below:

- Information pertaining to an individual who is not a potential match to a TSDB record will be retained for one year after the PANYNJ SWAC Program has notified TSA that the individual no longer has or is seeking access to PANYNJ restricted information, documents, or critical infrastructure assets.
- Information pertaining to an individual who may originally have appeared to be a match to a TSDB record, but who was subsequently determined not to be a match, will be retained for seven years after completion of TSDB matching, or one year after the PANYNJ SWAC Program that submitted the individual's information has notified TSA that they no longer have or are seeking access to PANYNJ restricted information, documents, or critical infrastructure assets, whichever is later.
- Information pertaining to an individual who is determined to be a positive match to a TSDB record will be retained for ninety-nine years after completion of matching activity,[2] or seven years after TSA learns that the individual is deceased, whichever is earlier.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information is retained for longer than necessary.

Mitigation: TSA will retain these records in accordance with the records retention schedule approved by NARA. The retention schedule was developed to provide flexibility to accommodate recurrent vetting during the time that the individual has access to the transportation facility, asset, or information, and to accommodate seasonal workers who may return annually. Retention of actual watch list matches mirrors the retention by the TSC, so there are no additional risks to the individual posed by TSA retention.

Privacy Risk: There is a risk that PANYNJ does not inform TSA of terminated employees in a timely fashion.

Mitigation: The risk is mitigated by drawing data directly from PANYNJ system rather than requiring affirmative conduct by PANYNJ. TSA data will be as current as the PANYNJ system.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

[2] See JUSTICE/FBI-019 Terrorist Screening Records System (TSRS) at http://www.fbi.gov/foia/privacy-act/72-fr-47073.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information on matches and potential matches will normally be shared with the TSC to confirm the match analysis and for operational response. Information is provided to TSC via password-protected e-mail. TSA will not share match information with PANYNJ.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS/TSA-002 Transportation Security Threat Assessment System of Records (TSTAS), 75 FR 28046 (May 19, 2010), Routine Use I permits disclosure "to the appropriate Federal, State, local, tribal, territorial, foreign, or international agency regarding individuals who pose, or are suspected of posing, a risk to transportation or national security." This is compatible with the collection of information for purposes of conducting security threat assessments since the TSC is the agency that maintains the TSDB and may coordinate an operational response if appropriate.

6.3 Does the project place limitations on re-dissemination?

No, TSA does not place limitations on re-dissemination of information by the TSC except to the extent match information is Sensitive Security Information pursuant to 49 U.S.C. § 114(r). Re-dissemination of SSI is limited by the SSI regulation, 49 C.F.R. Part 1520.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures to the TSC are recorded both manually within investigative files and automatically in an output report.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be inappropriately shared.

Mitigation: TSA may share this information in accordance with the Privacy Act. TSA mitigates attendant privacy risk by sharing externally only in accordance with published routine uses under the Privacy Act. Further, TSA has entered into an MOU with the FBI and TSC governing the conditions of sharing information. TSA will not provide the PANYNJ with any information or status from the TSDB check.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to their data under the Privacy Act by contacting the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020. Access may be limited pursuant to exemptions asserted under 5 U.S.C. §§ 552a(j)(2), (k)(1), (k)(2), and (k)(5).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

To correct inaccurate or erroneous PII submitted by the PANYNJ SWAC Program, affected individuals should request that the submission be updated by the PANYNJ SWAC Program with correct information. Once updated with the corrected information, the affected individual is resubmitted back through the TSA process. In addition, they may submit a Privacy Act request as described in 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

TSA does not have direct interaction with the individual. The PANYNJ will notify the individual that his or her PII is being submitted to TSA. This PIA provides notice on how to correct information held by TSA, however, TSA does not notify PANYNJ or the individual of the result of the TSDB check.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have an opportunity to correct, access, or amend their records maintained by TSA.

Mitigation: Individuals have an opportunity to check their data when it is submitted to PANYNJ, and can also update their information as needed within the SWAC. Any updates will be part of the daily data that TSA accesses. In addition, individuals may seek access to TSA records by submitting a request under the Privacy Act, though some aspects of their record may be exempt from access.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

System administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. Program management was involved in the conduct and approval of this PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All users are required to complete TSA-mandated Online Learning Center (OLC) courses covering privacy. In addition, security training is provided, which helps to raise the level of awareness for protecting PII being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002 (FISMA), Pub.L.107-347.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All access requests are submitted to the administrators of the TSA Consolidated Screening Gateway in writing and individual access is granted by an authorizing official. Access to any part of the system is approved specifically for, and limited only to, users who have an official need for the information in the performance of their duties. External storage and communication devices are not permitted to interact with the system. All access to, and activity within, the system are tracked by auditable logs. Audits will be conducted in accordance with TSA Information Security guidelines.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

New information sharing, uses or access will be controlled in accordance with sections 8.2 and 8.3, and will be reviewed for compliance with this PIA.

Responsible Officials

Joseph Salvator
Office of Intelligence & Analysis
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

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