Privacy Impact Assessment
for the

TSA Workplace Violence Prevention Program

March 30, 2010

Contact Point
Ted Calhoun
Program Manager, Workplace Violence Prevention Program
Office of Law Enforcement
Ted.Calhoun@DHS.GOV

Reviewing Officials

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) is committed to providing a safe work environment for its personnel. Toward that goal, TSA has established a Workplace Violence Prevention Program that provides: national guidance to TSA program coordinators regarding the prevention of, and response to, incidents of actual or alleged workplace violence; reviews reports of credible threats or actual incidents of workplace violence; provides advice and guidance to program coordinators and management regarding agency action; and coordinates training for program coordinators and TSA employees and contractors. Workplace Violence incident data, including personally identifiable information (PII), is maintained and secured by TSA program personnel.

Overview

TSA is committed to providing a safe work environment for all TSA employees and contractors, and enforcing the standards of personal safety and welfare at the workplace. Credible threats that are made against TSA employees, contractors, or TSA facilities may arise from individuals including other employees, contract personnel, former employees, or other members of the public. The Workplace Violence Prevention Program covers such threats, where such actions arise from or otherwise affect TSA operations. Examples may include, but are not limited to actual or implied threats, bullying or verbal abuse, repeated and/or inappropriate references to death, suicide, violence, assassinations, or acts of terrorism, physical contact against another person, acts of intimidation including brandishing a weapon (real or fake), or intentionally frightening employees, frequent and/or excessive displays of anger such as punching a wall or kicking equipment, throwing or striking objects, damaging or destroying property (including sabotage, computer viruses), and stalking.

Because this program entails a new analysis of information that may include members of the public in an identifiable form, the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0 Characterization of the Information

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

TSA will collect information about individuals involved in incidents of actual or alleged workplace violence as aggressor, victim, or witness. The information collected may include such information as full name, aliases and nicknames, date of birth, Social Security number, age, sex, physical description, telephone number, home and business addresses, time and attendance,

investigative information including video or audio recordings, medical or mental health information, counseling, and applicable court records including restraining orders.

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

The sources are individuals involved in workplace violence, investigators, or law enforcement personnel.

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

TSA collects this information to assist in coordinating prevention, notification, and response to incidents or threats of workplace violence.

1.4 How is the information collected?

TSA employees, investigators, or law enforcement collect information via paper format, telephonically or electronically to program personnel.

1.5 How will the information be checked for accuracy?

TSA will investigate incidents of actual or alleged workplace violence in order to assess the appropriate agency response. Information is checked for accuracy during the investigation.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Aviation and Transportation Security Act, 49 USC §114 provides general authorities for assessing threats against transportation and carrying out such other duties as appropriate relating to transportation security according to 5 U.S.C. § 301.

Once DHS has collected the information, it is governed by the Privacy Act of 1974, 5 U.S.C. § 552a.

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

The privacy risk associated with the collection of this information is the possibility of inappropriate dissemination of PII. In instances where PII is relevant or necessary to be collected, it will be protected so that only those individuals with appropriate access and a need to know will be able to review the PII collected.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

TSA uses the information to respond to alleged or actual incidents of workplace violence, to provide management oversight on TSA workplace violence and to provide training to TSA employees and contractors on the TSA workplace violence prevention program.

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

No tools are used to analyze data. Trend data may be developed through review by program personnel.

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

The program does not use commercial data, but may use publicly available data to find contact information for individuals involved in an incident.

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.

In instances where collection of personal information is necessary, it may only be viewed by appropriate personnel with the correct user roles. This ensures that privacy and information safeguarding requirements are met by limiting access to sensitive information, such as personal information, only to those users whose operational role and mission warrants such access.

Section 3.0 Retention

3.1 What information is retained?

TSA will retain all information about individuals involved in workplace violence. The information collected may include such information as full name, aliases and nicknames, date of birth, Social Security number, age, sex, physical description, telephone number, home and business addresses, time and attendance, investigative information including video or audio recordings, medical or mental health information, counseling, and applicable court records including restraining orders.

3.2 How long is information retained?

TSA expects to submit a records schedule to the National Archives and Records Administration (NARA) seeking to retain records for seven years after final agency administrative action following an incident. Records will not be destroyed until NARA approves a schedule.

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

Not yet.

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

The proposed retention period is reasonable given the propensity for workplace violence incidents to develop over time. It is similar to the seven year retention in NARA General Record Schedule 1 for employee grievance, disciplinary and adverse action files.

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?

The information may be shared with DHS employees and contractors who have a need for the information in the performance of their official duties. It is expected that information typically will be shared with TSA employees or contractors in the Office of Security Operations, Office of Law Enforcement, Office of Chief Counsel, and Office of Inspection. By way of further example, information may also be shared with the Office of Privacy Policy & Compliance, the Ombudsman, or the Office of Civil Rights and Civil Liberties in order to respond to individual complaints. To respond to congressional inquiries, the information may be shared with the Office of Legislative Affairs. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

4.2 How is the information transmitted or disclosed?

Information may be transmitted in paper format, electronically or telephonically.

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.

The privacy risk associated with sharing this information is the opportunity for improper dissemination of PII to individuals who do not have authority to receive or access the information. To mitigate this risk, TSA will only share this information with TSA and DHS employees and contractors who are authorized access and have a need for the information to perform their official duties in accordance with the Privacy Act. 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 access controls, including 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 organization(s) is the information shared, what information is shared, and for what purpose?

TSA may share information outside of DHS in accordance with the Privacy Act and the routine uses identified in the Workplace Violence Prevention Program System system of records notice (SORN). Routine uses include disclosing information to individuals or agencies when a person poses a threat of harm to himself/herself or others; to agencies or employers when relevant to an individual's employment; and to agencies responsible for investigating or prosecuting violations of law or regulation.

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. The information is shared in accordance with Privacy Act system of records notice (SORN) DHS/TSA 023, Workplace Violence Prevention Program, principally routine uses F, G, and I.

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

TSA shares information outside of DHS in paper format, electronically or telephonically, depending on the threat of harm for violence and the need to rapidly share the information. TSA MD 3700.4 governs the handling and transmission of sensitive PII including requirements for encryption and other safeguards.

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

The privacy risks associated with the sharing of this information is the possible dissemination of PII to unauthorized external entities. This risk is mitigated by TSA limiting the sharing of this information to those who have an official need to know it and by sharing only in accordance with published routine uses or under the Privacy Act.

Section 6.0 Notice

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

Information is typically collected through other TSA employees and there is no opportunity for notice to the individual involved in the workplace violence incident. When individuals seek assistance from workplace violence prevention program personnel, notice may be provided. If information is collected as part of a criminal investigation, notice is not provided.

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

In some instances, an individual has the right to decline providing PII. By way of example, an individual seeking advice from program personnel may decline to provide information. For personal information that may be associated with an investigation into a workplace violence incident, there is no opportunity to decline to provide information.

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.

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.

Workplace violence information is typically obtained through other TSA personnel or law enforcement and reported to workplace violence prevention program personnel. There is no risk that an individual seeking assistance or advice from workplace violence personnel are unaware of the information collection. There is a risk that other individuals involved in a workplace violence incident are initially unaware of the collection. Those individuals become aware of the information collection during the investigation that follows.

Section 7.0 Access, Redress and Correction

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

For individuals seeking access to their information in the system, such persons 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, East Tower
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?

Individuals can submit a request to correct records under the Privacy Act.

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

The TSA FOIA page, accessible through the TSA public website, contains a link permitting any individual to send information to TSA via a designated email address reserved for

that purpose. The FOIA page also contains a fax number and a mailing address for the same purposes for those who prefer to use those means to contact TSA.

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

Individuals have the right to present information as part of the investigation into a workplace violence incident.

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

If an individual believes that he or she has suffered an adverse consequence related to the system, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the system regarding a particular incident, activity, transaction, or occurrence.

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?

Workplace Violence Prevention program data is currently stored in a database accessed by the program director. Database access may expand to include other workplace violence prevention program personnel. IT specialists may be granted access as needed to perform functions related to software or hardware maintenance.

8.2 Will Department contractors have access to the system?

Yes, information technology contractors will have access to the system for software and hardware maintenance.

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

All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management for remedial action. In addition, all government and contractor personnel must complete annual information technology security training as required by FISMA.

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

Yes. Certification and Accreditation for End User Computing was completed and the Authority to Operate was granted in April 2009.

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

Role-Based Access Safeguards. The system technology will safeguard information by limiting a user's ability to view or update particular fields of information based upon the user's role.

Auditing Measures. Whenever data is entered, updated, or viewed, a record of that activity is captured and maintained within the system and can be retrieved and audited based upon the user or the record.

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?

The privacy risk associated with access and security controls is the unauthorized or inappropriate access of data in the system or access to the facility. Current risk is extremely limited, with only a single user having access to the program database. Expanded access is expected to be limited to program personnel. The data in 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.

Section 9.0 Technology

9.1 What type of project is the program or system?

The Workplace Violence Prevention program is operational. The database is a commercial off-the-shelf application which has been purchased for use by TSA to develop a database which will allow for recording and retrieving incident data.

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

The system is currently in the operational stage. No project development lifecycle was used.

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

No.

Approval Signature Page

Original copy signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security