Privacy Impact Assessment
for the

Crew Member Self Defense Training (CMSDT) Program

February 6, 2008

Contact Point
Michael Rigney
Federal Air Marshal Service
Flight Programs Division
Michael.Rigney@dhs.gov

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@tsa.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Department of Homeland Security Transportation Security Administration (TSA) has developed the Crew Member Self-Defense Training Program (CMSDT), a voluntary self-defense training course, for air carrier crew members. TSA will collect name, last 4 numerals of the Social Security Number (SSN), contact information, employer information including employee identification number, and course location preferences in order to verify a crew member's eligibility for the program and to provide the self-defense training. Because the CMSDT collects personally identifiable information (PII) on members of the public, TSA is conducting this Privacy Impact Assessment (PIA) in accordance with the statutory requirements of the E-Government Act of 2002.

Introduction

The Transportation Security Administration (TSA) has developed and implemented the CMSDT Program in order to comply with section 603 of the Vision 100 – Century of Aviation Reauthorization Act (P.L. 108-176) which requires TSA to make available a voluntary program of self-defense training for crew members of air carriers providing scheduled passenger air transportation. TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) is responsible for administering the CMSDT and has developed a training approach that combines distributed learning technology with hands-on instruction in self-defense techniques. Crew members interested in the training can get information from the TSA website, identify a training site, and register with the point of contact listed for the training site. Upon completion of self-paced instruction, an eligible crew member can attend a one-day, hands-on training session in self defense techniques applicable to the aircraft environment. In order to maintain proficiency, eligible crew members may repeat the training as many times as they would like. These one-day courses are conducted at select community colleges located throughout the United States, under a Cooperative Agreement with the American Association of Community Colleges (AACC).

Crew member information is collected by each individual AACC site coordinator. The collected information is then forwarded to a TSA contractor for employment verification. Once the contractor has verified the crew member's position and status with their respective employing airline, a confirmation is sent by the TSA contractor to the site coordinator authorizing the crew member's participation in the requested class.

TSA plans to collect limited PII from crew members seeking to participate in the CMSDT Program. This information will be gathered in order to (1) verify a crew member's eligibility to participate in the program; (2) register or re-register crew members for training classes; (3) allow crew members to receive the necessary instructional materials; (4) confirm and record crew members' attendance at a training class; (5) receive voluntary feedback from crew members regarding the quality of the instruction, instructors, and facilities used to deliver the training, and (6) provide crew members with information about recurring and/or advanced self defense training opportunities.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

Participating colleges will collect a crew member's name, address, telephone number, e-mail address, last 4 numerals of SSN, the name of their employing air carrier, their air carrier identification number, employee identification number, and the location of the community college at which they intend to participate in or directly observe the "hands-on" portion of the training, and will provide the information to TSA.

1.2 From whom is information collected?

The personal information is collected by participating colleges directly from crew members seeking this self-defense training. Crew members will provide the requested information to program coordinators at the community colleges sponsoring the CMSDT Program. A portion of the information (name, last 4 SSN, employing air carrier information) will then be provided to a TSA contractor for the purpose of conducting employment verification checks to confirm the crew member's eligibility to participate in the CMSDT Program.

1.3 Why is the information being collected?

The information is being collected for the purpose of verifying a crew member's eligibility to participate in the training program; managing their course enrollment and scheduling; maintaining control and security of the program's pre-course training materials; monitoring and assessing the quality of the program's training content, instructors, and facilities, and keeping participants informed of recurring and/or advanced self-defense training opportunities. Last 4 SSN is collected because some airlines require SSN for employment verification.

1.4 How is the information collected?

Participating community colleges will collect the necessary information directly from the crew member, and transmit it directly to TSA and the TSA contractor performing the employment verification checks. Information is collected on paper forms and through electronic registration, and may also be submitted by phone or fax.

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

Congress directed TSA to develop and implement a voluntary crew member self-defense training course in the Vision 100 – Century of Aviation Reauthorization Act, P.L. 108-176. To meet this obligation, TSA developed the CMSDT Program and partnered with AACC to implement the program. TSA and AACC have entered into a Cooperative Agreement which further describes and defines the partnership.

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

TSA has limited its collection to information necessary to verify crew members' eligibility for the training and administer the program. The information is used to accurately communicate identity with the employing airlines. Limiting the collection of information received by TSA to these minimal elements serves the agency's operational purposes and statutory mandates while minimizing the privacy risks to the program's participants.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the information to verify the eligibility status of crew members seeking to participate in the program; schedule crew members for training classes at participating community colleges; distribute instructional materials to eligible participants; verify the identity of the crew member at the training site; create a record of training participation; produce certificates of training completion, and advise participants of recurring and/or advanced training opportunities. Aggregate data not involving PII may be used to measure program performance.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Participating community colleges will collect the necessary information directly from the crew member, and transmit it directly to TSA and the TSA contractor performing the employment verification checks.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Since the community college collects the personal information directly from the individual to whom it pertains, the risk of collecting inaccurate information is minimized. Individuals can correct any inaccurate or changed employer, identification, or contact information at any time during the training.

Section 3.0
Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with record schedules once approved by the National Archives and Records Administration (NARA). TSA seeks to retain eligibility records for 3 years and class rosters for 3 years from the date of most recent application. The retention period allows TSA to prioritize training rosters in the event of limited class space.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

TSA does not yet have a record retention schedule approved by NARA for records pertaining to this program and must retain these records until such schedule is approved.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information collected in connection with this program will be maintained in accordance with NARA-approved record retention schedules. Risks associated with retention include data security issues that are mitigated by collecting information that has little value to someone that obtains the information without authorization.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The information collected will be accessed by those TSA employees and contractors who have a need to know the information in order to carry out their official duties. In the ordinary course, it is expected that CMSDT information will remain within OLE/FAMS and its contractor. This information may also be shared with other DHS employees in accordance with the Privacy Act, 5 U.S.C. § 552a.

4.2 For each organization, what information is shared and for what purpose?

TSA only receives information pertaining to crew members that are seeking to participate in the CMSDT Program. The information will be shared with TSA employees and contractors conducting employment verification checks in order to confirm a crew member's eligibility to participate in the

CMSDT. TSA may share that information within DHS for official purposes related to transportation security in accordance with the provisions of the Privacy Act 5 U.S.C. §552a.

4.3 How is the information transmitted or disclosed?

Depending upon the specific situation and need, the information may be disclosed telephonically, electronically via a secure data network or approved electronic data storage media, or via facsimile. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information is shared within DHS with those individuals who have a need for the information in the performance of their duties in accordance with the Privacy Act. Privacy protections include strict access controls such as 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?

In the ordinary course, TSA will share information with community colleges participating in the program in order to schedule the training. In addition, TSA expects to share information with employer airlines to verify training eligibility and provide training status. TSA may share individual information with others as permitted by the Privacy Act and in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/All-003, Department of Homeland Security General Training Records.

5.2 What information is shared and for what purpose?

Individually identifying data may be shared with participating colleges and employers to verify eligibility for training, schedule training, and report on the status of training.

5.3 How is the information transmitted or disclosed?

The information may be disclosed in person, telephonically, electronically via email or approved electronic data storage media, or via a facsimile.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

The CMSDT Program is administered pursuant to a Cooperative Agreement with the American Association of Community Colleges (AACC). This Agreement, along with the accompanying Statement of Work (SOW), fully reflects the scope of the information currently shared. A revised SOW, which will serve to implement revisions to the training delivery, also reflects the scope of the information shared.

5.5 How is the shared information secured by the recipient?

Under the CMSDT Cooperative Agreement, AACC is required to handle the information in accordance with the Privacy Act and take measures to protect information that comes into their possession as a result of this program.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No training of users outside DHS is required by TSA. However, TSA requires the information to be handled in accordance with the Privacy Act.

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

TSA will limit sharing of this information under the applicable provisions of the SORN and the Privacy Act. By limiting the amount of information collected, and sharing of this information to those who have an official need to know, TSA is mitigating attendant privacy risks.

Section 6.0
Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Applicants are given a Privacy Act Statement at the "Registration Information" section of the program website, as well as on the CMSDT Program Information Release Authorization form. See Appendix A. The publication of this PIA and of the SORN (DHS/All-003, Department of Homeland Security General Training Records), also serves to provide public notice of the collection, use, and maintenance of this information.

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

The CMSDT Program is voluntary, and crew members have an opportunity to decline to provide information in deciding whether or not to participate. However, an individual will not be provided with the program's instructional materials, nor allowed to directly observe or participate in the training unless they provide information that enables TSA to verify their identity and employment status.

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

No. All uses of the information obtained by TSA will be consistent with the Privacy Act and the applicable SORN.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Individuals are presented with a Privacy Act Statement on the program's website containing registration information, as well as on the release for those employers requiring a release to provide employment status. This informed consent coupled with the limited amount of personally identifiable information being collected effectively minimizes privacy risks associated with this 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 access their personal information by filing a Freedom of Information/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration

Freedom of Information Act Office, TSA-20

11th Floor East Tower

601 S. 12th Street

Arlington, VA 22202

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. The FOIA/PA request must contain the following information: Full name, address,

telephone number, and e-mail address (optional). Please refer to the TSA FOIA website at http://www.tsa.gov/research/foia/index.shtm.

7.2 What are the procedures for correcting erroneous information?

An individual may contest information maintained in the system that pertains to them by writing to the CMSDT Program Manager, or by contacting the participating college. The request must describe what information in the records is incorrect and why, with any supporting documentation. Individuals may also request correction of their personal information in this system of records in accordance with the applicable provisions of the Privacy Act and the DHS Privacy Act regulation at 6 C.F.R. § 5.26.

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

The publication of this PIA and of the SORN serves to provide public notice of the collection, use, maintenance, and means of correcting this information.

7.4 If no redress is provided, are alternatives available?

Although redress is provided, as described above, individuals will also have an opportunity to correct their information at the training site. In verifying the identity of the crew member at the training site, the college point of contact will review the crew member's personal information, and make corrections (such as spelling, contact information, and employing air carrier).

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Risks to privacy have been minimized by allowing individuals to correct the personal information they provide at the training site or facility. Further, individuals may request access to or correction of their personal information pursuant to the procedures outlined in this PIA and in accordance with DHS procedures for requesting amendment of records at 6 C.F.R. § 5.26.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

TSA does not currently operate and maintain a consolidated, automated system for processing and storing PII. Accordingly, system interaction is expected to be limited. Data related to crew members will only be accessed by TSA personnel with a need to know in order to perform their official duties. The information will be maintained securely on TSA's IT infrastructure, to which no public access is provided, and 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 officials.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

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. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. All contractors are subjected to requirements for suitability and a background investigation.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Role-based access controls are used for controlling access to the system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

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

Limited system access will be provided for purposes of managing this information. Generally, the system is secured against unauthorized use through a layered, defense-in-depth security approach involving procedural and information security safeguards.

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel are vetted and approved access to the data center where the system is housed, issued picture badges, and given specific access to areas necessary to perform their job function. A rules of behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the rules of behavior prior to getting access to any IT system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the system based on their function. TSA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained on information security when they join the organization and periodically thereafter. The Information Systems Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

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

The system is continuously monitored to audit compliance with policy. Weekly logs are reviewed to ensure no unauthorized access has taken place. All IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office.

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

All TSA employees and contractors are required to complete on-line TSA Privacy Training, which includes instructions on handling PII in accordance with the Privacy Act. Compliance with this requirement is audited monthly by the TSA Privacy Officer.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in TSA's record systems is safeguarded in accordance with the 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 legal authority of the Designated Accrediting Authority (DAA). Certification and Accreditation for FAMS Net was completed on December 8, 2005, and for Central Information Distribution System on October 27, 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

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. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system was built from Commercial Off the Shelf (COTS) products and customized applications. System components include COTS hardware and operating systems.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were analyzed based on FIPS-199 methodology. FIPS-199 methodology categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The result of that analysis was that the system was rated HIGH for data integrity and availability. All security controls are applied in accordance with this rating.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA had limited its data collection to specific elements necessary for confirming eligibility to participate in the program. TSA has developed an information technology infrastructure that will protect against inadvertent use of PII. The record system will include a real-time audit function to track access to electronic information, and any infractions of information security rules will be addressed appropriately. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuse.

9.4 Privacy Impact Analysis: What design choices were made to enhance privacy?

These conscious design choices will limit access to the personal information, thereby mitigating possible privacy risks associated with this program.

Conclusion

TSA is establishing this program to fulfill a statutory requirement to provide self defense training to crew members of commercial air carriers. Privacy impacts associated with this collection have been

minimized by limiting the breadth of information provided to TSA. TSA is only collecting the information necessary to verify program eligibility; facilitate training; maintain a record of individual training activity; and provide information regarding recurring and/or advanced self defense training opportunities. By limiting the scope of this collection, TSA has effectively minimized any privacy risks associated with the program.

Responsible Officials

Michael Rigney
Federal Air Marshal Service
Flight Programs Division

Approval Signature Page

_____

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

PRIVACY ACT STATEMENT: **Authority**: 49 U.S.C. § 114, E.O. 9397 (SSN). **Principal Purpose(s)**: To authorize TSA to obtain information from your employer in order to verify your employment status and approve you for participation in the Crew Member Self Defense Training Program. **Routine Use(s)**: This information may be shared with educational institutions or training facilities for the purpose s of enrollment and verification of attendance and performance, or for routine uses identified in the Department of Homeland Security's system of records notice, DHS/ALL-003 Department of Homeland Security General Training Records. **Disclosure**: Voluntary: failure to furnish this requested information may result in an inability to approve you for participation in the Crew Member Self Defense Training Program.