Privacy Impact Assessment
for the

# Canine Website System
# (CWS System)

## DHS/TSA/PIA-036

## January 13, 2012


**Contact Point**
**Carolyn Y. Dorgham**
**Program Manager, National Explosives**
**Detection Canine Team Program**
**Transportation Security Administration**
**Carolyn.Dorgham@dhs.gov**

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

## Abstract

Under the Aviation and Transportation Security Act (ATSA), the Transportation Security Administration (TSA) is responsible for security in all modes of transportation.[1] TSA's National Explosives Detection Canine Team Program (NEDCTP) prepares dogs and handlers to quickly locate and identify dangerous materials that may present a threat to transportation systems. The NEDCTP operates the Canine Website System (CWS), which is a web-based system designed to assist in coordinating operations. The CWS is the central management database for all NEDCTP records and operations. The CWS collects personally identifiable information (PII) to facilitate training, foster communication, and to perform administrative functions. Because this program entails a new collection of information by TSA about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 require that the TSA conduct a Privacy Impact Assessment (PIA).

## Overview

The NEDCTP is a partnership between TSA, airports, and local law enforcement agencies. The NEDCTP supports TSA's mission by preparing canine teams (handlers plus canines) to serve in support of transportation security initiatives. These canine teams locate and identify dangerous materials that may present a threat to transportation security. TSA uses the Canine Website System (CWS) to establish the initial CWS login ID and password, coordinate canine handler training, arrange initial travel and reimbursement, create team profiles, perform annual certifications, conduct evaluations of the amount of time dedicated to screening cargo, provide information identifying the aircrafts that teams train on, and other administrative functions. In addition, the CWS also provides a means of communication among TSA Headquarters, field staff, and canine teams/local law enforcement agencies by providing a message forum, help desk, useful Internet links, travel and/or training documents and news.

The federal government does not employ canine handlers but trains them to perform transportation security operations. Canine handlers are employees of the state, county, city, or airport law enforcement authority designated to provide airport security. In order to participate in the program and to facilitate training and other administrative functions, canine handlers must submit PII, including their name, agency name, work, home, and mobile phone numbers, work and home addresses, email address, work telefax number, airport ID number and canine team name to TSA via the CWS. TSA uses this information to confirm the particular state, or local authority the officer works for, although a traditional background check is not conducted using this information. In addition, canine handlers may provide Social Security Numbers (SSN) and credit card information to the CWS system on a one-time basis to allow TSA employees to arrange access to the training facility, prepare their initial travel orders, and facilitate

[1] Pub.L. 107-71 (Nov. 19, 2001); 49 U.S.C. § 114 (f).

reimbursement. TSA trains canine teams at its Explosives Detection Canine Handler Course at Lackland Air Force Base in San Antonio, Texas. The canine handlers are also able to create personal profiles and biographies in the CWS system, which only contains the limited PII the handlers choose to submit for profile purposes. TSA also collects the name and contact information of the canine handlers' respective supervisor and trainer in the team profile.

Upon designation as a canine team by the state, county, city, or airport law enforcement authority, TSA grants the canine handler web-based access to the CWS system. The canine handler submits the PII contained in Section 1.1 to TSA via the CWS system in order to initiate the required NEDCTP training, create travel orders and reimbursement, build his or her personal profile, and facilitate other administrative functions. Upon completing the travel order, TSA deletes the SSN and credit card information but stores the remainder of the information contained in Section 1.1. This information includes the individual's name, employment information (i.e., airport ID, agency and canine team name), work and home addresses, work, home, and mobile phone numbers, work telefax numbers, and email address as part of the team profile. TSA also uses this information to establish the initial CWS login ID and password for each handler. In order to facilitate annual evaluations and certifications, TSA will store canine handler training records in CWS. Since the canine handler's agency prepares and funds all subsequent travel and reimbursement requests, TSA has no need to retain the canine handler's SSN and credit card information after the initial NEDCTP training. Should the operational need arise for TSA to facilitate and fund subsequent canine handler travel and reimbursement, the individual shall resubmit their SSN and credit card information to TSA for processing on a case-by-case basis. Only the canine handler, their agency canine unit supervisor, and the CWS system administrator can access the data TSA maintains.

## Section 1.0 Characterization of the Information

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

Typically, the CWS collects the following information from canine handlers:

- Name;
- SSN and credit card information solely for the purposes of arranging access to the training facility, prepare their initial travel orders and to facilitate reimbursement;
- Gender (used for lodging accommodation purposes);
- Agency name;
- Work, home, and mobile phone numbers;
- Home and work addresses;

- Email address;
- Work telefax number;
- Airport identification number and name of canine team;
- Biography (voluntary); and
- Training Records.

In addition, TSA collects the name and contact information of the canine handler's supervisor and trainer for the purpose of creating a team profile in the system that can be viewed only by the canine handler, his or her agency canine unit supervisor, and the CWS system administrator.

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

TSA collects the information directly from canine handlers seeking to participate in the program. This includes the name and contact information of their respective supervisor and trainer associated with the state, county, city or airport law enforcement authority designated to provide airport security.

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

TSA collects information to coordinate canine handler training, arrange facility access, travel and reimbursement, establish a CWS login ID, create personal and/or team profiles and directories, facilitate the annual certification and evaluation processes, and foster communication and other administrative functions.

### 1.4 How is the information collected?

TSA collects the information electronically through the CWS. Canine handlers that are accepted into training must complete a web-based form. The Chief of the NEDCTP (or his/her authorized designee) approves all access requests to the CWS system. Canine handlers who are granted access to CWS can only access their own profile and information using their unique login ID and password.

### 1.5 How will the information be checked for accuracy?

Because the individual submits the information directly, the data entered is presumed accurate. If inaccurate, the individual may access the system at any time to correct the information contained in his or her profile or contact the administrators of the CWS for assistance in correcting any other information.

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

Pursuant to 49 U.S.C. § 114, TSA is responsible for security in all modes of transportation. TSA is also responsible for providing for the screening of all passengers and property (49 U.S.C. § 44901). In addition, each participating state, county, city, and airport law enforcement agency signs a Cooperative Agreement with TSA. The Cooperative Agreement outlines roles and responsibilities for all parties involved. TSA collects the information pursuant to 49 CFR Part 18, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments. Additionally, the following Office of Management and Budget (OMB) Circulars are applicable to this Cooperative Agreement:

1. OMB Circular A-87 (05/04/1995) (further amended 08/29/1997) Cost Principles for State, Local and Indian Tribal Governments;

2. OMB Circular A-102 (10/07/1994) (further amended 08/29/1997) Grants and Cooperative Agreements with State and Local Governments; and

3. OMB Circular A-110 Common Rule for Uniform Administrative Requirements for Grants and Other Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations.

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

TSA considered the risk related to the amount of information obtained and limited the collection to the data listed in Section 1.1. in order to facilitate travel, training and to perform administrative activities. TSA limits the information collected from individuals to specific contact information necessary to facilitate NEDCTP training and other administrative functions, as well as limits system access to the canine handler, his or her agency canine unit supervisor, and the CWS system administrator. To mitigate the risk of exposing canine handler sensitive PII used to provide initial travel orders and reimbursement, TSA deletes the SSN and credit card information from the CWS database after preparation of the initial travel order. Additionally, all TSA employees and contractors receive privacy and security official training.

## Section 2.0 Uses of the Information

### 2.1 Describe all the uses of information.

TSA uses the information to contact individuals, coordinate canine handler training, arrange facility access, travel and reimbursement, establish a CWS login ID, create personal and/or team profiles and directories, facilitate the annual certification and evaluation of canine

handlers, and other administrative functions. TSA also uses the data entered into the CWS to capture the time dedicated to screening cargo as entered by the handlers, training times, and to identify aircraft used for team training. Further, TSA uses this information to confirm the particular federal, state, or local authority the officer works for, although a traditional background check is not conducted using this information.

In addition, canine handlers provide SSNs and credit card information to the CWS system on a one-time basis to allow TSA employees to arrange access to the training facility, prepare their initial travel orders, and facilitate reimbursement. Since the canine handler's agency prepares and funds all subsequent travel and reimbursement requests, TSA has no need to retain the canine handler's SSN and credit card information after the initial NEDCTP training. Should the operational need arise for TSA to facilitate and fund subsequent canine handler travel and reimbursement, the individual shall resubmit their SSN and credit card information to TSA for processing on a case-by-case basis.

### 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.

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

No commercial or publicly available data is used by the CWS system.

### 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 risk presented by the use of contact and travel-related information is that the information would be used in ways outside the scope intended by the initial collection. All TSA employees and contractors are trained on the appropriate use of PII. Further all releases of information are done in accordance with the Privacy Act System of Record Notices (SORNs) described in 5.1 below.

## Section 3.0 Retention

### 3.1 What information is retained?

TSA retains the PII contained in Section 1.1.

### 3.2 How long is information retained?

Canine handler information collected to facilitate CWS access will be maintained in accordance with NARA-approved record schedules under General Record Schedule (GRS) 20. TSA will delete the SSN and credit card information from the CWS database after processing the initial travel order and reimbursement. Once TSA's record schedule has been approved by NARA, TSA will destroy/delete the remaining information in Section 1.1 15 years after completion or suspension of training.

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

No. TSA submitted the CWS records retention schedule to NARA for review on September 20, 2011.

### 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 privacy risk associated with the length of time that CWS data is retained is that the information may become vulnerable to unauthorized use or PII disclosure. To mitigate the risk of retention of PII associated with the maintenance of the CWS system, individuals who no longer wish to participate in the program may request that the information be deleted by notifying their agency of their decision. The agency's representative must contact the portal operator to request removal of the canine handler's account. TSA will then terminate the account and no longer retain the member's limited contact information, thereby reducing privacy risks posed by retention of their contact information. Retaining the information in accordance with the NARA-approved GRS ensures that TSA adheres to the Fair Information Principle of minimization, which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

## 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?

Consistent with the Privacy Act and the DHS/ALL-003, DHS General Training Records (71 FR 26767, May 8, 2006) and DHS/ALL-004, General Information Technology Access Account Records System (GITAARS) (73 FR 28139, May 15, 2008) SORNs, information may be shared with employees that have a need to know the information in the performance of official duties. It is expected that information typically will be shared with TSA employees or contractors in the following TSA offices: Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Office of Security Policy and Industry Engagement, Office of Chief Counsel, Office of Intelligence and Analysis, Office of Security Operations, and Office of

Inspection. While it is not routinely shared outside of TSA, TSA may need to share information within DHS, specifically with the U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) in association with potential joint canine exercises or deployments.

**4.2 How is the information transmitted or disclosed?**

Information may be shared by electronic or paper means.

**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 it. To mitigate this risk, TSA will share this information only with DHS employees and contractors who have a need to know 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 strict 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?**

Information may be shared with external governmental entities inasmuch as those entities are involved in distributing information or collaborating with partners within DHS. Sharing with external entities is limited to the uses described in relevant SORNs, DHS/ALL-003, DHS General Training Records and DHS/ALL-004, GITAARS. TSA will also share the individual's SSN with the U.S. Air Force to arrange access to the training facility.

**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 contained in the CWS system may be shared with entities outside of DHS in accordance with the routine uses identified in the following Privacy SORNs, DHS/ALL-003 (71 FR 26767, May 8, 2006) and DHS/ALL-004 (73 FR 28139, May 15, 2008). TSA will also share the individual's SSN with the U.S. Air Force to arrange access to the

training facility. Specifically, TSA may share this information in accordance with the following Routine Uses:

DHS/ALL-003 Routine Use I allows DHS to share this information with educational institutions or training facilities for purposes of enrollment and verification of employee attendance and performance.

DHS/ALL-003 Routine Use L allows DHS to share this information with employers to the extent necessary to obtain information pertinent to the individual's fitness and qualifications for training and to provide training status.

DHS/ALL-004 Routine Use H allows DHS to share this information with sponsors, employers, contractors, facility operators, grantees, experts, and consultants in connection with establishing an access account for an individual or maintaining appropriate points of contact and when necessary to accomplish a DHS mission function or objective related to this system of records.

DHS/ALL-004 Routine Use I allows DHS to share this information with other individuals in the same operational program supported by an information technology system, where appropriate notice to the individual has been made that his or her contact information will be shared with other members of the same operational program in order to facilitate collaboration.

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

Information may be shared by paper or electronic means. Information shared with members of the CWS system is safeguarded by providing access controls so that only authorized members may access the portal's resources.

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

The privacy risk 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 in DHS/ALL-003 (71 FR 26767, May 8, 2006) and DHS/ALL-004 (73 FR 28139, May 15, 2008) or pursuant to disclosures permitted under the Privacy Act, 5 U.S.C. 552a(b).

## Section 6.0 Notice

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

Yes. Prior to each collection of contact information, TSA provides a Privacy Act Statement (see Appendix A) to individuals at the time they submit their information regarding the scope and purpose of the contact information at the time of collection.

Furthermore, this PIA and the SORNs listed in Section 5.1 provide notice regarding the collection of contact and travel-related information by TSA.

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

Yes. Individuals are not required to provide their information. However, if individuals do not provide their information, they will not be able to obtain an account to access the CWS system.

In addition, canine handlers provide SSN and credit card information to the CWS system on a one-time basis to allow TSA employees to arrange access to the training facility, prepare their initial travel orders, and facilitate reimbursement. Since the canine handler's agency prepares and funds all subsequent travel and reimbursement requests, TSA has no need to retain the canine handler's SSN and credit card information after the initial NEDCTP training. Should the operational need arise for TSA to facilitate and fund subsequent canine handler travel and reimbursement, the individual shall resubmit their SSN and credit card information to TSA for processing on a case-by-case basis.

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

Yes. Individuals have the ability to consent to particular uses of some information. Specifically, CWS publishes a member directory and individuals may opt-out of or limit the information published.

### 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.

Individuals voluntarily register to become a member of the CWS system in order to facilitate operational activities, collaborate and exchange information with other members; thus individuals are well aware of the purpose for the collection. In addition, notice is provided to the user regarding the uses of their information upon registering to the portal. This PIA provides further notice to individuals, as do the SORNs listed in Section 5, and the Privacy Act Statement attached in Appendix A that is provided to individuals.

## Section 7.0 Access, Redress and Correction

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

After receiving their initial login ID and password, individuals seeking to access or edit their information, may either log on to the CWS system or contact the CWS system administrator for assistance. Individuals seeking to remove their information may contact the CWS system administrator to remove his or her information.

Individuals may also 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 visiting the TSA Submitting FOIA Requests page (http://www.tsa.gov/research/foia/foia_requests.shtm). 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/research/foia/index.shtm.

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

Generally, individuals may log on directly to the CWS system to correct any inaccurate information about them or update their contact information. If the individual cannot directly correct their record, the CWS system administrator is in the best position to correct any inaccurate information. Individuals may also request that information pertaining to them be corrected through the DHS FOIA/Privacy Act process described in section 7.1.

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

Individuals are notified at the time of collection that they may correct their information by the procedures outlined above.

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

Formal redress is provided through notice and ability to change/edit, or remove information.

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

The privacy risk associated with redress is the collection of inaccurate information. This risk is mitigated by the individual's ability to correct his or her information either directly by accessing the CWS system, by contacting the CWS system administrator, or through the FOIA process.

## 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?

The state, county, city or airport law enforcement authority designated to provide airport security determines who is eligible to become a member of the CWS system. TSA uses field coordinators to contact canine program stakeholders to verify potential members during the registration process to ensure they are authorized to use the portal. Upon successful completion of the registration process, users may access the CWS. In terms of administration of the system, DHS physical and information security policies dictate who may access DHS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to Department computers which is where the majority of contact information is stored. 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.

### 8.2 Will Department contractors have access to the system?

Yes. Many times contractors are tasked with either development or administration of the system. Contractors are required to have the same level of security clearance as all other DHS employees in order to access TSA computers.

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

All TSA employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of sensitive PII.

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

Yes. The CWS system received an authority to operate on March 18, 2009.

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

All TSA information systems are audited regularly to ensure appropriate use and access to information. Authorized users must supply a valid log-in and password to obtain access to CWS system. Within TSA, access to system resources and member information is limited to those who require it for completion of their official duties. CWS system administrators periodically review shared spaces to ensure that postings by its members do not contain sensitive PII or PII about those who are not members or potential members of the online community. Administrators have the ability to remove any inappropriate postings.

### 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 to data in the system. To mitigate risks against unauthorized or inappropriate access to the system, TSA implements access controls and restricts the collection of PII to a limited set of contact and travel-related information used to facilitate operational activities and collaboration among authorized members of the CWS system. Access to the system by TSA employees and contractors is limited to those who have a need to know the information in the performance of their official duties. Further, TSA conducts thorough background checks on every employee and contractor. Additionally, all TSA employees and contractors receive privacy and security training.

## Section 9.0 Technology

### 9.1 What type of project is the program or system?

The CWS system is a web-based system used to facilitate NEDCTP operational activities and communication with canine program stakeholders.

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

The program or projects detailed here are not necessarily involved in a specific lifecycle. Complete information technology systems are in the operational phase and have completed C&A documentation. Individual contact information lists do not have a development cycle.

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

With the exception of the SSN and credit card information used for initial canine handler travel orders and reimbursement, no technology used here raises specific privacy concerns. TSA deletes the SSN and credit card information upon completion of the travel orders. CWS system members have the ability to post comments, links, and documents but the content of these postings should not contain sensitive PII. Members are instructed specifically not to post PII to shared spaces. In addition, CWS system administrators periodically review shared spaces to ensure that sensitive PII is not posted and have the ability to remove inappropriate member postings.

## Responsible Officials

Carolyn Dorgham
Program Manager, National Explosives Detection
Canine Team Program
Transportation Security Administration

## Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

## APPENDIX A

**Privacy Act Statement:**

**Authority:** 49 U.S.C. § 114(f) authorizes the collection of this collection.

**Purpose:** DHS will use this information will be used to coordinate canine handler training, arrange initial travel and reimbursement, establish a Canine Website (CWS) login ID, create team profiles and directories, perform annual certifications, and conduct evaluations of the mandatory amount of time dedicated to screen cargo, and other administrative functions.

**Routine Uses:** The information will be used by and disclosed to appropriate federal, state, local or tribal governmental agencies for law enforcement, intelligence, or security purposes, or to airports or air carriers to facilitate canine program operations. This information is shared in accordance with the Privacy Act and the routine uses identified in the DHS General Training Records System of Records Notice (SORN), DHS/ALL-003 (May 8, 2006, 71 FR 26767), and the General Information Technology Access Account Records System (GITAARS) System of Records (SORN), DHS/ALL-004 (September 29, 2009, 75 FR 49882-49885).

**Disclosure:** Furnishing this information is voluntary; however, failure to provide the requested information could result in the canine handler's inability to join the program or gain access to the CWS.