1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

a. Date PIA was completed: March 26, 2010

b. Name of system: Defense Trade Application System

c. System acronym: DTAS

d. IT Asset Baseline: 199

e. System description (Briefly describe scope, purpose, and major functions):

The Defense Trade Application System (DTAS) is a system provided to U.S. citizens and specified foreign individuals who submit license applications for the export or temporary import of defense articles and defense services pursuant to the International Traffic in Arms Regulations (ITAR). It also provides for the storage and distribution of licensing and compliance information and facilitates the activities of License and Compliance Officers and their teams.

f. Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

g. Explanation of modification (if applicable):

h. Date of previous PIA (if applicable):

June 8, 2008

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Personally identifiable information (PII) is collected in DTAS on all applicants. The following is a list of all collections and the PII gathered for each:

- Statement of Registration (Form DS-2032)
  - Name
  - SSN
  - DOB
  - Place of Birth
  - Home contact information
  - Business contact information
- Electronic Forms (Forms DSP-5, DSP-61, DSP-73, DSP-119)
  - Name
  - Business contact information
- Paper Forms (Forms DSP-6, DSP-62, DSP-74, DSP-83, DSP-85, DSP-94, DS-4071, DS-6000, DS-6001, DS-6002, DS-6003, DS-6004)
  - Name
  - Business contact information
- Data from Legacy System
  - Name
  - Address
  - SSN
  - Alien Registration Number
  - DOB
  - Place of Birth
  - Home contact information
  - Business contact information
- License Application Information
  - Name
  - Business contact information

Sources of this information are the forms listed above. Each form is completed by the applicant him/herself.

b. How is the information collected?

Information is collected by applicants completing forms listed in section 3a above. Each form has a Privacy Act Statement for the notification of the record subject. Once the form is completed, it is either uploaded into DTAS, or the information is manually entered by a DTAS Department of State employee.

c. Why is the information collected and maintained?

Due to the sensitive nature of its purpose (collecting and storing licensing information for those seeking to import or export defense articles or services), DTAS collects PII on all applicants. The information collected on licensing forms is then passed on to other Federal agencies (i.e. the Department of Defense, NASA, and DHS) for a referral. These agencies make their recommendations on whether or not to grant the license, and this recommendation is used in the Directorate of Defense Trade Controls' (DDTC) final decision. After it is combined with information from a daily feed from the Census Bureau, it is passed along to Customs and Border Protection (CBP), where they check it against their information to ensure that the export or import is allowed to leave or enter the country.

DDTC collects PII from Form DS2032 to establish a registrant's bona fides and their eligibility to export and temporarily import defense articles. The PII collected on the registration form is shared with Immigration and Customs Enforcement in order for them to conduct a law enforcement check, a requirement in determining eligibility.

d. How will the information be checked for accuracy?

All information from individuals is collected on Department of State forms and entered into DTAS by system users. Although users look for errors when entering the information, there really is not a way for the record subject to check his or her information for accuracy once he or she submits it via the forms listed in 3a.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

Section 38 of the Arms Export Control Act (AECA), 22 U.S.C. 2778-2780, authorizes the President to control the export of defense articles and defense services. Additionally, the AECA requires all companies and individuals that manufacture and/or export/temporarily import defense articles to register. Part of the registration process involves a law enforcement check conducted by Immigration and Customs Enforcement. The statutory authority of the President to promulgate and administer regulations with respect to exports of defense articles and defense services was delegated to the Secretary of State by Executive Order 11958, as amended. The International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130, implements that authority. By virtue of delegations of authority by the Secretary of State, these regulations are administered by the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs, Department of State.

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

Due to the nature of PII collected in DTAS, it can be classified as a “moderate” level system. As this system collects license applications from those who seek to export or import defense articles or services, its dealings with PII are appropriate. When personal information is sent to CBP, only the person’s name and business contact information is used, and information is collected directly from the record subject by forms containing a Privacy Act statement. The amount and type of PII collected is appropriate for the purpose.

4. Uses of the Information

a. Describe all uses of the information.

In order to obtain license transaction information, the DTAS user receives a flat file from the Automated Export System (AES) data set from the Census Bureau. This information is then formatted in DTAS, transferred to diskette, and hand carried to a dedicated dial-up workstation where it is sent to CBP via an emulated RJE connection. CBP uses the information for law enforcement concerns and advises DDTC about potential issues or problems regarding eligibility or export law violations. They compare it to their records to ensure that the record subject can export or import defense articles. In addition, the information collected from the record subject is stored in DTAS as a record of who has requested a license for compliance purposes.

b. What types of methods are used to analyze the data? What new information may be produced?

The data collected is not, itself, analyzed. Instead, it is used to verify the identity of the record subjects applying for licenses to export or import defense articles or services and ensure they are allowed to export or import weapons.

No new information is produced within DTAS.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

No commercial information, publicly available information, or information from other Federal agency databases is used in DTAS.

d. Are contractors involved in the uses of the PII?

Contractors are involved in the input of information into DTAS, as well as the maintenance of the system. All contractors have undergone extensive training on proper usage of the DTAS system and are monitored by federal employees.

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

The DTAS system is designed to collect and maintain information on those who are required to register with the Department and request a license to export or temporarily import defense articles or services. As a result, data analysis is simple, and no commercial information, publicly available information, or information from other Federal agency databases is used in the system. This creates a negligible risk that the information may be used for other than the intended purpose. Other regulations include access agreements for users of DTAS, security and privacy awareness training, and system use notifications (warning banners).

5. Retention

a. How long is information retained?

Records stored in DTAS follow various retention schedules based on the sensitivity of the information collected or the necessity of retention. The records disposition schedules used are A-24-048-01a(1) – 01d(2). The records schedules are mandated as follows:

- PKI protected Application Forms, Contract or Purchase Orders, Certificates of Compliance, in-house and other agencies' clearances, and technical reference materials describing the export product should be deleted after input and verification of data into master files or when no longer needed to support the creation or reconstruction of the master file, whichever is later.
- For paper Arms Export Case Files, their cutoff should be after the issuance of the license and in the case of ITAR registration files, cutoff is after expiration of the registration code. They should be retired to the Records Service Center after the cutoff and transferred to the Washington National Records Center (WNRC) when they are five years old. After 20 years, they should be destroyed.
- Master files in DTAS are cut off after the issuance of a license or expiration of the registration code. Case files are maintained online and retired to the Records Service Center when no longer needed for current operations. They are deleted 20 years after cutoff.
- Screens of information related to completed forms are deleted after provided to a user.
- Ad-hoc and periodic reports produced in electronic or hardcopy media against any of the data elements and in any arrangement are deleted/destroyed when superseded by an updated or new report.
- CD-ROM backup copies of files are deleted when superseded by an updated copy.
- External and internal user manuals prepared to provide descriptive and technical documentation related to the use of DTAS are destroyed/deleted when superseded or one year after the termination of the system.

- System managers manuals prepared to provide documentation needed to understand the operations of the system are destroyed/deleted when superseded or one year after termination of the system.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The DTAS system retains PII on applicants for purposes of registration and for licenses for defense articles or services. The records disposition schedules above ensure that records are only kept as long as necessary. DTAS system owners follow the schedules as best they can, ensuring that information is expunged after a reasonable amount of time.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information from DTAS is not shared with any internal organizations.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information from DTAS is not shared with any internal organizations.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Since information from DTAS is not shared with any internal organizations, no privacy risk results.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

As mentioned in sections 3 and 4 above, some information gathered in DTAS is shared with CBP, ICE and AES. However, the only information shared is name and business contact information. The purpose of this external sharing is to obtain licensing transaction information from the Bureau of Census, which is then consolidated with DoS information and sent to CBP. The latter checks this information against their records to ensure that the record subjects are allowed to export or import defense articles.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Once the Census Bureau compiles their information daily from the AES data set, it is sent as a flat file to a DTAS user. This information is then formatted by a DTAS user. The name and business contact information of the record subjects and information from the Census Bureau is transferred to diskette and hand carried to a dedicated dial-up workstation where it is sent to CBP via an emulated RJE connection. For registration PII, on-site ICE liaison officers review hard copies of registration forms and compare data with information resident in a law enforcement database, accessible via secure telecommunication lines.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Though external sharing can be even riskier than internal sharing at times in terms of privacy concerns, minimal and non-sensitive PII is shared externally through DTAS. The result is a negligible privacy risk.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

STATE-42, Munitions Control Records

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Each of the forms used to collect personal information from record subjects contains a Privacy Act statement. These forms are compliant with section e(3) of the Act.

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

Due to the nature of the collection of information for DTAS, the record subject does not have the opportunity or right to decline to provide information. All information collected is needed to ensure that all record subjects are who they say they are and that they are allowed to export or import defense articles.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, the record subject does not have a right to consent to limited, special, and/or specific uses of the information. All information is needed for the purposes set out in 8(b).

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

Notice is provided to record subjects in the above-mentioned SORN. In addition, no privacy risk results from the extent to which DTAS does or does not offer options to record subjects in storing their PII in the system.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Due to the nature of the purpose of the DTAS system, record subjects are not allowed to access their information for amendment. However, the record subject provides personal information on him or herself in the initial collection, so he or she has a chance to make sure all information is correct. In addition, record subjects must notify DDTC by registered mail within five days of an

event if there are material changes in the information contained in registration (Form DS-2032) submissions.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

This category of privacy risk is minimal, as the record subject provides the personal information, and very limited PII is shared outside of the users of DTAS.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to DTAS requires a username and password that are only granted after the user completes extensive training on using the system and licensing. All users of DTAS are employees or contractors of DTTC of the Department of State and must have a justified need for the information in order to perform their official duties. To access the system, the user must be an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Access control lists, which define who can access the system, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. Each user is also required to take a yearly computer security and privacy awareness training prior to accessing the system. Given all of these safeguards, this category of privacy risk is low.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

No technologies commonly considered to elevate privacy risk are employed in DTAS.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

As the technologies used are standard and contained on a government-operated platform, the privacy risk for this category is negligible.

12. Security

a. What is the security certification and accreditation (C&A) status of the system?

DTAS has a C&A authorization in place through May 2010, and steps have been taken to start the recertification process.