

DEPARTMENT OF STATE
PRIVACY IMPACT ASSESSMENT
FOR
DEFENSE TRADE APPLICATION SYSTEM

Conducted by:
Bureau of Administration
Information Sharing and Services
Office of Information Programs and Services
E-mail: pia@state.gov

A. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: pia@state.gov . If answer is yes, please complete the survey in its entirety.**

YES NO

*The following are examples of personally identifiable information:

- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

To support the regulation of the commercial sales/transfer of defense equipment and technology to foreign persons.

3) What legal authority authorizes the purchase or development of this system/application?

Section 38 of the Arms Export Control Act (22 U.S.C. 2778) authorizes the President to control the export of defense articles and defense services. 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 CFR 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.

C. DATA IN THE SYSTEM:

- 1) Does a Privacy Act system of records already exist?**

YES NO

If yes, please provide the following:

System Name: Munitions Control Record; State-42

If no, a Privacy system of records description will need to be created for this data.

2) What categories of individuals are covered in the system?

Persons (individuals as well as corporations, business association, partnerships, societies, trusts, or any other entities, organizations or groups, including governmental entities) who engage in the business of either manufacturing or exporting defense articles or furnishing defense services or engage in arms brokering.

3) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

For the most part, the source of personally identifiable information is provided from the persons described above. Some other information may be provided by U.S. Government sources, such as law enforcement agencies.

b. Why is the information not being obtained directly from the individual?

If there is a violation of U.S. export law or a conspiracy to violate that law, information about the suspects or violators are mostly likely to come from other sources.

c. What Federal agencies are providing data for use in the system?

In most instances, other agencies do not provide the initial personally identifiable information that is contained or reflected in the DDTC system. Rather, in general, their information would be used to supplement or verify the information that is collected from persons described in C2 above.

d. What State and/or local agencies are providing data for use in the system?

N/A

e. From what other third party sources will data be collected?

N/A

f. What information will be collected from a State Department employee and the public?

Personally identifiable information most commonly relates to a legal requirement for the persons described in C2 above to register with the Department of State. Registrants must submit documentation that demonstrates they are incorporated or otherwise authorized to do business in the United States. A letter is required stating whether the registrant and/or senior officers have ever been convicted of violating certain U.S. criminal statutes (enumerated in section 120.27 of the ITAR) or is ineligible to contract with, or to receive an export/import license of other U.S. Government agencies. The letter must also state whether the registrant is owned or controlled by foreign persons. Other personally identifiable information required in a Registration Statement includes names, home addresses, nationality, and social security numbers of senior officers.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

All registration information is reviewed by Department of Homeland Security (DHS)/Customs.

b. How will data be checked for completeness?

The information is reviewed at several levels by DDTC's Office of Defense Trade Controls Compliance.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Registrants must, within five days of the event, notify DDTC by registered mail if there are material changes in the information contained in Registration Statement submissions.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. Registration Statement (Form DS-2032).

D. DATA CHARACTERISTICS:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. Applications for licenses or other export approvals are considered only if the applicant has registered with DDTC. Export approval is linked closely with the eligibility of persons to participate in U.S. defense trade transactions.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

When this occurs, the Office of Defense Trade Controls Compliance will modify, as appropriate, records on Registration or compliance and enforcement cases.

3) Will the new data be placed in the individual's record?

In virtually all cases, this information would be placed in the registration record.

4) Can the system make determinations about employees/public that would not be possible without the new data?

The system does not make determinations about participants in defense trade. Information is input into the system that allows DDTC officers to determine factors such as eligibility and legitimacy of certain business transactions.

5) How will the new data be verified for relevance and accuracy?

The new personally identifiable information, for the most part, would be verified and provided by federal or local law enforcement agencies or, at the very least, reviewed by DHS/Customs in the course of the Registration process.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The system is not physically accessible outside of the DDTC proper. Internal controls (DS compliant lockdowns, audit logs, etc.) ensure individuals only access information needed for their specific job function.

Consolidation of information within the system would still enjoy the protection of section 38(e) of the Arms Export Control Act and section 126.10 of the ITAR, under which information required by the Department by registrants and export authorization applicants may generally not be disclosed. Internally, System Access rules and policy support need-to-know access. Users of the system are allowed to view and manipulate only data they are authorized to see.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

The system is not physically accessible outside of DDTC. Separation of authority and established roles and responsibilities preclude unauthorized individuals from being involved in data processes outside of their scope of work.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The corresponding System of Records Notice for this system is Munitions Control Records; STATE-42. Computerized searches can be made against names of persons or their corporate affiliates.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Computerized searches can be made against names of persons or their corporate affiliates. Results are sometimes used in criminal court certifications or periodic civil compliance audits. Records access is restricted to authorized DDTC personnel. Access or manipulation of records is electronically monitored and can be traced to the user.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is not operated at more than one site.

2) What are the retention periods of data in this system?

In accordance with the September 2002 Records Disposition Schedule for DDTC, the cutoff for Registration files is when the registrant is no longer required to be registered; retirement to the Records Service Center is one year after cutoff. Destruction of records is scheduled 25 years after cutoff.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The corresponding System of Records notice for this system is Munitions Control Records; STATE-42.

All electronic records will be maintained in a manner equivalent to their corresponding paper records, which are filed with the records retirement center in accordance with the Department's Records Disposition Schedules.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

There is no significant effect to public/employee privacy.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system is specifically designed to identify persons described in C.2 above as the identification relates to regulated defense trade transactions.

7) What kinds of information are collected as a function of the monitoring of individuals?

DDTC's focus is the monitoring/regulation of defense export transactions that fall under U.S. jurisdiction rather than the monitoring of Persons per se.

8) What controls will be used to prevent unauthorized monitoring?

The system does not track this type of activity; however, audit trails and periodic IT security reviews are used to ensure proper access of system data by users.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No.

11) Are there forms associated with the system? YES NO

If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Yes.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)

The data will be accessed by contractors, DDTC staff (users), system administrators, and software developers.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Everyone within the DDTC office with access to the system has access to all data on the system. This is required due to the collaborative business process flow used to conduct the Directorate's business.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

There are no "users" other than the DDTC staff members. The system has no direct connectivity out of the facility. All users are authenticated to the system prior to use and "need-to-know" access is managed through assignment of operational roles.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

System audit trails are maintained and periodically reviewed to detect unauthorized access attempts. Unauthorized "browsing" of data by users cannot take place since everyone connected is authorized access and may from time to time need access to any or all of the stored data. The system is monitored by system administration staff for unusual activity on a routine basis.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Contractors are and will be involved. No specific Privacy Act training has been provided to support contractor staff.

The Task Order contract has a paragraph (quoted below) requiring the contractor to not divulge information in connection with the task order.

6) Do other systems share data or have access to the data in the system? If yes, explain.

Personally identifiable information, other than description of defense export transactions, is not shared through other systems.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Security for data resident on other agency systems will be the responsibility of that agency's Policy Automation Directorate (PAD) Security Administrator (SA), who will serve as the single point of contact of contact within the agency for general access and automation issues related to the DDTC system.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

Personally identified information (PII) is reviewed, pursuant to law, by DHS/Customs.

9) If so, how will the data be used by the other agency?

DHS/Customs looks at the data for law enforcement concerns and advises DDTC about potential issues/problems regarding eligibility or export law violations.

10) Who is responsible for assuring proper use of the data?

DDTC is the "owner" of the data. Agencies with whom data is shared must subscribe to "third agency" rule and other data protections such as the Privacy Act.