

Submit the completed PIA to
[Privacy's SharePoint Customer Center](#)

Privacy Impact Assessment for the Defense Trade Application System

1. Contact Information

<p>A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services</p>

2. System Information

- (a) Name of system: Defense Trade Application System (DTAS)
- (b) Bureau: PM/DDTC
- (c) System acronym: DTAS
- (d) iMatrix Asset ID Number: 199
- (e) Reason for performing PIA: Reauthorization
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Modified for new template.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

Yes

No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

Expired in 1/2016. Reauthorization submitted to IRM/IA on 12/18/2015.

(c) Describe the purpose of the system:

The Defense Trade Application System (DTAS) is the tool by which the Directorate of Defense Trade Controls (PM/DDTC) adjudicates license applications submitted by U.S. citizens and specified foreign individuals for the export or temporary import of defense articles and defense services pursuant to the International Traffic in Arms Regulations (ITAR). Additionally, DTAS provides for the storage and distribution of licensing and compliance information and facilitates the activities of License and Compliance Officers and their teams.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The following chart outlines each PII item collected by DS or DSP form. Each form is completed by the applicant him/herself. No PII is collected from other federal agency systems. An “X” delineates that this form collects the corresponding PII data, regardless of quantity or whether the PII is significant or insignificant.

DTAS Personally Identifiable Information Types by Form

PII Type (Individual or Business)	DS-2032	DS-4076	DSP-5	DSP-6	DSP-61	DSP-62	DSP-73	DSP-74
Names of Individuals I	X	X	X	X	X	X	X	X
Birthdates of Individuals I	X	None	None	None	None	None	None	None
Financial Account Numbers I/B	X ¹	None	None	None	None	None	None	None
Social Security Number(s) I	X	None	None	None	None	None	None	None
Phone Numbers of Individuals I	X	X	X	X	X	X	X	X
Names of Business(es) B	X	X	X	X	X	X	X	X
Business Address(es) B	X	X	X	X	X	X	X	X
Personal Address(es) I	X	None	None	None	None	None	None	None
Email Address(es) of Individuals I	X	X	X	X	X	X	X	X
Images or Biometric IDs I	None	None	None	None	None	None	None	None

Substantive Individual Information – Medical	I	None	None	None	None	None	None	None	None
Substantive Individual Information – Financial	I	None	None	None	None	None	None	None	None
Substantive Individual Information – Legal	I	None	None	None	None	None	None	None	None
Substantive Individual Information – Personnel	I	None	None	None	None	None	None	None	None
Substantive Individual Information – Family	I	None	None	None	None	None	None	None	None
Substantive Individual Information – Educational	I	None	None	None	None	None	None	None	None
Substantive Individual or Business Information – Other	I/B	None	X ²	X ³					

¹Partial only – ²Potential business Intellectual Property and/or sales data – ³Substantial third party names, addresses, phone numbers

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

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 ICE. 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) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: STATE-42 SYSTEM NAME: Munitions Control Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
March 20, 2008

No, explain how the information is retrieved without a personal identifier.

The information is searchable by a company record number

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No

(If uncertain about this question, please contact the Department’s Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-24-048-01
- Length of time the information is retained in the system: Up to five years; retire to NARA up to 25 years.
- Type of information retained in the system:

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). These schedules mandate 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 5 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 1 year after the termination of the system.
- System managers manual prepared to provide documentation needed to understand the operations of the system are destroyed/deleted when superseded or 1 year after termination of the system.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes No

- If yes, under what authorization?

22 U.S.C. 2651A (Organization of Department of State)

5 U.S.C. 301 (Departmental Regulations)

22 U.S.C. 2778 (Arms Export Control Act).

Executive Order 13478 (Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers)

(c) How is the information collected?

All PII is collected by IBM or Adobe form and transmitted securely through the DDTC external web site(s) using modern cryptographic technologies. Section 3(d) lists the specific forms used to collect the information.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

- If you did not select "Department-owned equipment," please specify.

Click here to enter text.

- (e) What process is used to determine if the information is accurate?
Manual review and verification is performed by the DDTC License Officers in accordance with DDTC policy and procedures.
- (f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Yes. DDTC information and data is reviewed and updated frequently by DoS Specialists specifically tasked with these responsibilities. Information is processed, verified, adjudicated, and archived as appropriate.
- (g) Does the system use information from commercial sources? Is the information publicly available?
No – all information is input by DDTC stakeholders only. These stakeholders include government staff, contractors, and industry users.
- (h) Is notice provided to the individual prior to the collection of his or her information?
Yes, notice is presented on all websites, including DTrade and DTAS-online. The “Privacy Notice” is a hyperlink which forwards a user to the following U.S. Department of State “Privacy Policy” (<http://www.state.gov/misc/415.htm>). Additionally, 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 Privacy Act. In addition, State-42 provides notice to individuals of the collection of PII in DTAS.
- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?
 Yes No
 - If yes, how do individuals grant consent?
Individuals click on the “agree” button on the application webpage. Due to the nature of the collection of information in DTAS, the record subject cannot conduct business with DDTC if they 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.
 - If no, why are individuals not allowed to provide consent?
Click here to enter text.
- (j) How did privacy concerns influence the determination of what information would be collected by the system?
Personal information is required for PM/DDTC to complete its mission. The usage of private information (PII) is required to obtain all relevant and pertinent information in order to verify and validate each external customer as part of the registration process. The least amount of personal information is collected in order to accomplish the PM/DDTC mission.

5. Use of information

(a) What is/are the intended use(s) for the information?

The information is collected to provide data and metrics for review by appropriate USG agencies in order to fulfill export control requirements.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is relevant and only the minimum amount of information is collected.

(c) Does the system analyze the information stored in it? Yes No

If yes:

(1) What types of methods are used to analyze the information?

[Click here to enter text.](#)

(2) Does the analysis result in new information?

[Click here to enter text.](#)

(3) Will the new information be placed in the individual's record? Yes No(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? Yes No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Registration information gathered in DTAS is shared with the Department of Homeland Security (DHS). DHS staff receive hard-copies of registration application packages for clearance by law enforcement after downloading registration applicant information from a secure FTP site.

The Department of Defense (DoD) receives electronic copies of license application packages for technical review of license applications by subject matter experts at these agencies (USXPORTS). In addition, approved license and registration information is sent to Customs and Border Protection (CBP) to allow this agency to verify if a license provided with a shipment is valid and to check license information against their records for the purpose of determining if record subjects are allowed to export or import defense articles. Personal information provided to CBP includes all data elements collected as part of the business entity registration.

(b) What information will be shared?

The following information is shared with external government agencies:

- Registration and License information, to include (as applicable):
 - Applicant (Registrant) information:
 - Applicant Nationality / Citizenship
 - Registrant Type (Manufacturer/Exporter/Broker(US Only))
 - New or Renewal Indicator
 - Manufacturer Registration Code
 - Broker Registration Code
 - Registrant Information
 - Registrant Legal Business Name
 - Registrant Doing Business As Name
 - Registrant Street Address
 - Registrant Phone
 - Registrant Fax
 - Registrant Website
 - Registrant is a US Affiliate Company Indicator
 - Registration Fees
 - Amount
 - Non Profit Fee Indicator
 - Name on Account
 - Payment Effective Date
 - FedWire/ACH/SWIFT
 - Last 5 Digits of the Account #
 - Trace or IMAD Number
 - Organizational Type (Corporation/Company/Limited Liability Company/Partnership/Individual Owner/Other)
 - Date of Incorporation
 - Place of Incorporation

- Principle Officer Information
 - Full Name (Last / First / Middle)
 - SSN or Equivalent (Permanent Resident Card Number)
 - Government Issued ID
 - Position Title
 - DOB
 - Place of Birth
 - Nationality / Citizenship
 - Home contact information (including address, telephone, fax (if applicable), and e-mail)
- USML (USML Defense Articles Involved in Manufacturing, Exporting or Brokering)
- Subsidiary Information
 - US or Foreign Indicator
 - Legal Business Name
 - Doing Business as Name
 - Street Address
 - Phone
- Indictment Status
 - Whether registrant had been indicted, charged, or convicted
 - Reinstatement Letter Attached indicator (Y/N)
- Contract License Eligibility
 - Eligibility Details
- Foreign Ownership
 - MoreThan50 (Ownership %)
 - Foreign Policy Maker Authority
 - MoreThan25 (Ownership %)
 - MoreThan5 (Ownership %)
 - Owned By Foreign Details
- Have Brokering Report
 - Supporting attachments

- Type
 - Third Party Point of Contact
 - Company Name
 - Name of Person
 - Phone
 - Email
 - Correspondence Email
 - Senior Official Name
 - Senior Officer Title
 - Senior Officer Email
 - Initial Registration Date
 - Registration Expiration Date
 - Expiration Month
 - Expiration Year
- (c) What is the purpose for sharing the information?

DHS

For purposes of background information and criminal record review

DOD

For technical review of license applications by subject matter experts at this agency as provided to USXPORTS

CBP

To verify if a license provided with a shipment is valid and to check license information against their records for the purpose of determining if record subjects are allowed to export or import defense articles

- (d) The information to be shared is transmitted or disclosed by what methods?

Information is shared only by secure transmission methods, such as SSL/TLS or SFTP.

- (e) What safeguards are in place for each internal or external sharing arrangement?

Each connection has a documented Memorandum of Understanding or Agreement, as well as an Interconnection Security Agreement as required.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The minimum amount of personal information is exchanged, and the MOU/A and ISPs (as listed above) outline the control requirements for all parties.

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?

There are no automated processes; individuals can request their information from the DDTC Service Desk. Individuals who have reason to believe that the Directorate of Defense Trade Controls might have records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA-2, Department of State, Washington, DC 20522-8001. The individual must specify that he or she wishes the records of the Directorate of Defense Trade Controls to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Directorate of Defense Trade Controls has records pertaining to him or her.

In order for registrants to access their information, a digital certificate must be issued to an empowered official and/or Senior Officer from a trusted third-party certificate authority to be managed on the user's internet browser and used to verify the user in addition to a username and password. The user must follow specific procedures to acquire and provide the digital certificate information to the DDTC Help Desk team through e-mail in order to complete the attestation process. Access to registrant / company data, are managed through permissions and roles within DTAS that are administered by the industry corporate administrator.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

Individuals may contact the DDTC Service Desk to correct any errors in their personal information. Service desk internal procedures ensure the integrity of all over-the-phone transactions.

If no, explain why not.

Click here to enter text.

- (c) By what means are individuals notified of the procedures to correct their information?

The main DDTC website (<http://pmdtcc.state.gov>) gives instructions on how to contact the service desk.

8. Security Controls

- (a) How is the information in the system secured?

The DTAS Information System is secured in accordance to a FISMA Moderate-impact system, with NIST 800-53 controls. These controls include technical protections such as advanced network firewalls, intrusion detection devices, government-approved encryption devices, and full auditing capabilities. Also included are administrative controls, such as policies and procedures to ensure data handling by authorized personnel only. These controls are assessed (audited) on a periodic basis by an independent office to ensure compliance.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

All employees of the Department of State have undergone a thorough personnel security background investigation. Access to the Department of State building and the annexes is controlled by security guards, and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured filing cabinets or in restricted areas, access to which is limited to authorized personnel. Access to electronic files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

All DTAS systems employ standard and customized auditing functionality. Per State 12 FAM 632.1, all audit logs are reviewed at least monthly by the ISSO.

- (d) Explain the privacy training provided to authorized users of the system.

The DTAS system relies on standard OpenNet information security training, including privacy, to reinforce the importance of safeguarding confidential data and PII.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? Yes No

If yes, please explain.

The information is secured using industry standard technologies, such as TLS encryption for data-in-transit and TDE encryption for the database(s). Access to information is restricted to approved users who have authorization to use DTAS.

(f) **How were the security measures above influenced by the type of information collected?**

The NIST SP 800-53 Moderate impact security baseline was selected to ensure proper protections for sensitive data and PII in DTAS. These controls and associated State Department Foreign Affairs Manual (FAM) policies were requirements to the overall system design and its ongoing operation. DDTC follows State policy and processes for ongoing monitoring and risk management.

9. Data Access

(a) **Who has access to data in the system?**

Department of State PM/DDTC employees and contractors with a business need are granted access based on their role and responsibilities. All personnel with access must complete State Department processing for a security clearance of Secret or higher. No vendors or other third-parties have access to the DTAS data. Applicants that submit information to DTAS are granted access to the system to view/modify/update information for their organization.

(b) **How is access to data in the system determined?**

For PM/DDTC personnel, system access needs are determined by role or position within DDTC. For organizations that submit registrations and licenses to DDTC, accounts are created with necessary permissions to support their associated business transactions. The primary point of contact at each submitting organization determines the additional accounts necessary for their organization and associated role.

(c) **Are procedures, controls or responsibilities regarding access to data in the system documented?** Yes No

(d) **Will all users have access to all data in the system, or will user access be restricted? Please explain.**

For PM/DDTC personnel user access is restricted by job function, role, position, and security clearance level. For submitting organizations, access is restricted to their organization's information submitted and associated responses from DDTC.

(e) **What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?**

Role-based access controls are implemented to ensure least privileges necessary are assigned to each user account based on authorized role. Accounts must be approved by the supervisor and system manager.

Auditing is enabled on the network, system and databases to record all user access attempts and actions performed. Periodic auditing is performed by Information System Security Officers to detect any policy violations or suspicious activity such as unauthorized browsing of data. If policy violation, suspicious activity or security incident is detected, it is reported immediately to the State Department Cybersecurity Incident Response Team. Following investigation, if warranted, disciplinary action up to and including termination (or contract cancellation) is possible.