

Privacy Impact Assessment for the Defense Export Control and Compliance System (DECCS)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

- (a) Name of system: Defense Export Control and Compliance System (DECCS)
- (b) Bureau: PM/DDTC
- (c) System acronym: DECCS
- (d) iMatrix Asset ID Number(s): 169761, 256970
- (e) Reason for performing PIA: DECCS is the replacement for existing Defense Trade Application System (DTAS).
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable):

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?

DECCS is a new information system. As of October 2017, the DECCS system is undergoing Department of State A&A processes. The Directorate of Defense Trade Controls (DDTC) anticipates completion of the required A&A processes resulting in grant of Authorization to Operate (ATO) by February 2018.

- (c) Describe the purpose of the system:

DECCS is used by DDTC to register entities involved in brokering, manufacturing, exporting, or temporarily importing defense articles or defense services enumerated on the U.S. Munitions List (USML); adjudicate requests for licenses or other authorizations; support determinations regarding requests for commodity jurisdiction determinations

(CJ); and to facilitate the issuance of requests for advisory opinions (AO). Entities using DECCS are U.S. citizens, corporations, and limited foreign individuals. Additionally, DECCS provides for the storage and distribution of licensing and compliance information and facilitates the activities of licensing, policy and compliance officers.

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

PII is collected in DECCS for all license applicants, but may not be required for all entities using DECCS. The following is a list of all PII collected by DDTC that is stored and processed in DECCS:

PII collected by DDTC:

- Entity Information (such as Applicant)
 - Name (First, Middle, Last)
 - Physical Address
 - City
 - State/Province
 - Country
 - Zip/Postal Code
 - Nationality
 - Passport Number
 - Visa Number
 - Operator / Certificate License (only for aircraft and vessel commanders)
 - Telephone
 - Email
 - Fax
 - Information related to current or past law enforcement charges and convictions, and
 - Contract and license eligibility.

- Mailing Address
 - Address
 - City
 - State/Province
 - Country
 - Zip/Postal Code

- Secondary Entity Contact Information
 - Name
 - Telephone

- Email
- 3rd Party Point of Contact (POC)
 - Name
 - Telephone
 - Email
 - Address
 - City
 - State/Province
 - Country
 - Zip/Postal Code
- Members of the Board of Directors, Senior Officers, Partners, and Owners of Parent Entity
 - First Name
 - Middle Name
 - Last Name
 - Social Security Number or Equivalent
 - U.S. Person – Yes/No
 - Citizenships
 - Place of Birth
 - Date of Birth
 - Birth City
 - Birth Country
 - Birth State/Province
 - Home Address
 - Address
 - City
 - State/Province
 - Country
 - Zip/Postal Code
 - Phone Number
 - Email

When necessary, this information is collected via OMB-approved forms to support DDTC business operations. Forms are completed and submitted by applicants. PII is also obtained by DDTC from systems operated by other federal agencies, specifically the U.S. General Services Administration (GSA) Integrated Award Environment (IAE) system known as the System for Award Management (SAM).

- (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, authorizes the President to control the import, export, and brokering of defense articles and defense services enumerated on the USML. Section 40A of the AECA, 22 U.S.C. 2785, directs the President to establish an end-use monitoring program for defense articles and defense services. The President delegated the AECA authorities in part to the Secretary of State by Executive Order 13637. The International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130, implements the Secretary's authority with respect to direct commercial sales. These regulations are administered by the DDTC, Bureau of Political-Military Affairs, in the 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 also 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 (N1-059-04-04)
- Length of time the information is retained in the system: Information is retained in DECCS for up to ten years.
- Type of information retained in the system: All information submitted to DDTC, including the PII listed in paragraph 3(d) of this document, will be retained in DECCS. Please refer to STATE-42 for more information regarding the specific information stored in DECCS.

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. 2778, 2785 (AECA section 40A).

(c) How is the information collected?

All PII is submitted through forms DSP-5, DSP-61, DSP-73, DSP-119, DSP-6, DSP-62, DSP-74, DSP-85 and DS-4076 that have been approved by the Office of Management and Budget (OMB). These forms are presented to the user via the DECCS web application transmitted using secure http (https) transport layer security (TLS).

(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.

The information is hosted in the Microsoft Azure Government Community Cloud Solution and the ServiceNow Government Cloud. Both of these cloud solutions have been accredited through the FedRAMP Joint Authorization Board and have received a Provisional Authorization to Operate (P-ATO).

(e) What process is used to determine if the information is accurate?

Authorized DDTC personnel and contractors conduct manual reviews to verify information submitted by industry users. DECCS service desk technicians review information related to the creation of DECCS user accounts belonging to DDTC personnel and contractors 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?

DECCS industry users are responsible for ensuring their company's information in DECCS is current. Changes to a company's registration or licensing information must be submitted in accordance with the ITAR. Information provided by external data sources are updated in DECCS on a weekly basis.

DDTC personnel or contractors must contact the DDTC service desk if their information must be updated in DECCS. The DDTC service desk personnel process tickets and address requested and approved changes following DDTC policy and procedures.

- (g) Does the system use information from commercial sources? Is the information publicly available?

No, all information is provided by DDTC stakeholders and is not from commercial sources or publicly available. These stakeholders include government staff, contractors, and industry users—both U.S. and foreign.

- (h) Is notice provided to the individual prior to the collection of his or her information?

Yes, notice, titled “Privacy Notice”, is presented at the bottom of each web page supporting DECCS.” 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 (5 U.S.C. 552a). In addition, the SORN, State-42, provides notice to individuals regarding the collection and storage of PII in DECCS.

DDTC users of DECCS are required to sign a DECCS access request form that includes the Privacy Notice listed above.

- (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?

- If no, why are individuals not allowed to provide consent?

The information requested by DDTC is required for DDTC to perform its statutory responsibilities. PII from each DECCS customer is required to manage access control to the system in accordance with Department of State policy and Federal Information Security Management Act (FISMA) federal guidelines. The PII collected from each DECCS customer is also required for DDTC to fulfill its mission of controlling the brokering, export, and temporary import of defense articles and services enumerated on the USML.

DDTC personnel and contractors who access DECCS must provide PII to create unique identities and accounts in the system. This information is required by Department of State policy and FISMA to manage access to federal information systems.

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

DDTC carefully examined data requirements to support its mission. Collection of PII is limited to that which is absolutely necessary to support DDTC business functions and interactions with industry / DECCS customers. DDTC drafts and obtains approval for collections of data from OMB following publication for public comment.

5. Use of information

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

Information collected thru DECCS will:

- Provide data to be used in the consideration of export control authorizations and associated functions to ensure transactions are consistent with foreign policy and national security;
- Provide metrics to be used for compliance and reporting purposes;
- Be used to grant system access to DECCS customers, DDTC personnel, and DDTC contractors.

- (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?

The data collected from DECCS customers is analyzed by DDTC staff to perform the functions listed on page 2 of this document in response to question 3c. Methods include individual analysis, group analysis, interoffice analysis, and interagency analysis.

- (2) Does the analysis result in new information?

The analysis conducted by DDTC staff and subject matter experts may result in new information including, but not limited to, determinations, registrations or licenses.

- (3) Will the new information be placed in the individual's record? Yes No

New information is associated with the entity for which the inquiry was submitted.

- (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.

- Department of State
 - Bureau of Administration (A)
 - Bureau of African Affairs (AF)
 - Bureau of Democracy, Human Rights, and Labor (DRL)
 - Bureau of Diplomatic Security (DS)
 - Bureau of East Asian and Pacific Affairs (EAP)
 - Bureau of European and Eurasian Affairs (EUR)
 - Bureau of International Security and Nonproliferation (ISN)
 - Bureau of Near Eastern Affairs (NEA)
 - Bureau of Political-Military Affairs (PM)
 - Bureau of South and Central Asian Affairs (SCA)
 - Bureau of Western Hemisphere Affairs (WHA)
 - Office of the Legal Advisor (L)
- Department of Commerce
 - Bureau of Industry and Security (BIS)
- Department of Defense
 - Defense Security Service (DSS)
 - Defense Technology Security Administration (DTSA)
- Department of Energy (DOE)
- Department of Homeland Security
 - Customs and Border Protection (CBP)
 - Homeland Security Investigations (HSI)
- Department of Justice
 - Federal Bureau of Investigation (FBI)
 - Offices of the United States Attorneys (USAO)
 - Counterintelligence and Export Control Section (CES)
- National Aeronautics and Space Administration (NASA)
- Other participating agencies of the Export Enforcement Coordination Center (E2C2)
- House Foreign Affairs Committee
- Senate Foreign Relations Committee

(b) What information will be shared?

Security event and audit data regarding access and use of DECCS resources and information will be shared with DS.

The PII listed in paragraph 3(d) will be shared with other U.S. Government agencies as necessary.

PII provided to the House Foreign Affairs Committee and Senate Foreign Relations Committee is limited to entity name.

(c) What is the purpose for sharing the information?

A: For the purposes of responding to Freedom of Information Act requests.

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

DS: To provide independent monitoring of system for security policy enforcement, malicious activity detection, and security incident response.

CES, HSI, FBI, E2C2, USAO: For purposes of background information and criminal record review, as well as investigatory and litigation purposes.

L: For legal consultation.

Other internal or external agencies: For technical review of license and commodity jurisdiction applications by subject matter experts to inform DDTC's decision-making process.

Senate Foreign Relations and House Foreign Affairs Committees: For review of licenses by congressional staffers as described in sections 123.15 and 124.11 of the International Traffic in Arms Regulations (22 CFR §§ 123.15, 124.11).

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

Information is shared by secure transmission methods including transport layer security (TLS) using secure FTP website access.

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

DDTC has an Information Sharing Agreement (ISA) with DHS/CBP and a Memorandum of Agreement (MOA) with DTSA. For all internal and external sharing arrangements, we provide the data that is needed to perform statutory and regulatory functions. The

agreed data sets are sent either via Secure File Transfer Protocol (SFTP) for DTSA and CBP, Password protected access to DTSA's USXPORTS system, Password protected SharePoint 365 for specific staff members of Congress and encrypted email for other external users. Internal users are provided password protected access to DTSA's USXPORTS system or are sent via internal email through Department of State controlled exchange servers.

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

Since DDTC collects PII and business sensitive data from regulated industry users, the data exchanges are performed pursuant to Department of State policy 12 FAM 640 Domestic and Overseas Automated Information Systems Connectivity, 12 FAM 053 Memorandum of Understanding and Agreements, and 12 FAH-10 H-700 File Transfer Procedures Using Removable Media. Security controls were selected and implemented from the NIST SP 800-53 Rev 4 control catalog for Moderate Impact system to include Privacy Controls contained in this NIST Standard. These controls protect the information systems, its connections, and implement monitoring. Further, PII and business sensitive data is shared with internal and external sources on a need-to-know basis, using Secure File Transfer Protocol, password protected system access, encrypted email for external users, and using required sensitivity markings to identify when PII is being transmitted.

7. Redress and Notification

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

There are no automated processes that support direct access to personal information by external entities who are not registered within DECCS. Individuals who have reason to believe that DDTC 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 would like DDTC's records 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 DDTC has records pertaining to him or her. An individual can also request their information from the DDTC Service Desk.

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 Service Desk through e-mail in order to complete the attestation process. Access to registrant/company data, is managed by the

person designated as the “corporate administrator” for each Industry served by DDTC. The permissions for the corporate administrator role within DECCS permit each authorized “corporate administrator” to manage the persons from their organization that are granted access to the organization’s information in DECCS.

- (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.

The ITAR requires certain changes to be reported to DDTC. These changes must be reported in accordance with the ITAR and the data collection approved by OMB for that purpose.

If no, explain why not.

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

The main DDTC website (<http://pmddtc.state.gov>) provides instructions on how to contact the service desk. State-42 and this PIA also provide notice to individuals.

8. Security Controls

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

Information in DECCS is secured in accordance with a FISMA Moderate-impact system by selecting and implementing security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls*, which is required for a Federal Information Processing Standards (FIPS) 199 Moderate impact system. Additional security controls were selected over the minimum baseline for a Moderate Impact system to address unique requirements for cloud computing systems. These controls span technical, operational and management aspects of information system design, administration and operation to protect the information in the system, monitor the system, and respond to security incidents when detected.

- (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.

Role-based access control is implemented across DECCS to ensure access is limited to the least privilege necessary to perform tasks based on the user’s organizational affiliation and role within the organization. DDTC personnel and contractors are granted rights and permissions via a role-based access control system to ensure that their access corresponds with the their job function and/or position. Industry users of DECCS will be

able to view information that they, themselves, submit. Access to other information related to their company will be denied unless the individual is granted such access by the company's point of contact.

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

All DECCS user actions and network data are included in log auditing functionality for analysis and reporting. System logging also includes all activity for external users, internal application users, and system administration users. Per State 12 FAM 632.1, all audit logs are reviewed at least monthly by the Information System Security Officer.

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

DDTC personnel and contractors are required to complete cyber security awareness training (Foreign Service Institute, PS800) that covers the procedures for handling Sensitive but Unclassified (SBU) information, including PII. Annual refresher training is mandatory and records of successful completion are managed by IRM/IA. DDTC personnel must also complete training for identifying and marking SBU information (Foreign Service Institute, PK323) in order to properly identify and label sensitive information in electronic mail, IT systems and in paper. Refresher training must be completed every two years or annually, depending on the employee's position and role in DDTC. This training will become mandatory for DDTC contractors in 2017 upon further instruction from the Department.

Industry users of DECCS are required to sign an agreement prior to obtaining access to the system. This agreement stipulates requirements of the industry organization to ensure its personnel complete annual cybersecurity and privacy training.

(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.

DECCS is built to meet the security controls required for a moderate-impact system. These security controls, specifically NIST SP 800-53 Rev 4, span all aspects of system design, implementation and operation to include encryption, identity and authentication.

All DECCS components and cloud services implement encryption algorithms and hashes compliant with FIPS 140-2, Security Requirements for Cryptographic Modules.

DECCS is configured to require strong authentication requiring multiple factors (userID and password along with another factor).

All communications between components and between user and system are protected using encryption. Data is also encrypted when at rest within DECCS.

- (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 SBU information and PII in DECCS. These controls and associated State Department Foreign Affairs Manual (FAM) 5 FAH-11 H-000 Information Assurance Handbook and 12 FAM 540 Sensitive But Unclassified Information (SBU) policies and handbooks were requirements for the overall system design and its ongoing operation. Additional security controls were selected to support processing of data using cloud services. DDTC follows State Department policy and processes for ongoing monitoring and risk management.

9. Data Access

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

DDTC personnel and contractors whose roles and responsibilities require access will have access to DECCS. Industry users that submit information to DECCS will have access to the system to view/modify/update information that they, themselves, submitted. Industry users will be able to access information related to their company, regardless of whether or not they submitted the information, if they are designated by their company to view such information.

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

System access for DDTC personnel and contractors is determined by an employee's clearance, position, and responsibilities. All DDTC personnel and contractors granted access to DECCS must be cleared at the secret level or higher. Furthermore, DDTC personnel and contractors who are granted access will be assigned permissions via a role-based access control system that corresponds with the employee's job function and position. Industry users who are not registered with DDTC, but who submit certain information to DDTC¹, will only be able to view information related to their submission. Industry users who are registered with DDTC may have access to their company's information (parent and subsidiary) at the company's discretion. The company's point of contact may grant or restrict access to its employees at any time.

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

¹ Request for Commodity Jurisdiction, Request for Advisory Opinion, Voluntary Disclosure, reexport or retransfer request, notifications, or a first time Statement of Registration.

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

Please explain.

User access for DDTC personnel and contractors is restricted based on the employee's level of clearance, position, and responsibilities. Industry users who are not registered with DDTC, but who submit certain information to DDTC, will only be able to view information relevant to their submission. Industry users who are registered with DDTC will—at most—only have access to information that is relevant to their company. This access may be further restricted by the user's company.

- (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. Monthly auditing is performed by the system Information System Security Officer to detect any policy violations or suspicious activity such as unauthorized browsing of data. If policy violation, suspicious activity or a 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.