PRIVACY IMPACT ASSESSMENT

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) Date of completion of this PIA: January 4, 2022
(b) Name of system: Defense Export Control and Compliance System
(c) System acronym: DECCS
(d) Bureau: Political-Military Affairs (PM)
(e) iMatrix Asset ID Number: 169761
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

DECCS is used by the Directorate of Defense Trade Controls (DDTC) in the Bureau of Political-Military Affairs (PM) to register entities involved in brokering, manufacturing, exporting, or temporarily importing defense articles or defense services enumerated on the U.S. Munitions List (USML); to adjudicate requests for licenses or other authorizations; to support determinations regarding requests for commodity jurisdiction (CJ) determinations; and to facilitate the issuance of requests for advisory opinions (AO).

DECCS provides interfaces for the submission, processing, reference, analysis and issuance of registration and license applications. DECCS allows DECCS users to complete the end-to-end registration and renewal processes online through a single, cloud-based portal.

Entities using DECCS (DECCS users) can be a natural person or limited foreign individual, as well as a corporation, business association, partnership, society, trust, or any other entity, organization, or group, including governmental entities.

In addition, DECCS provides for the storage and distribution of licensing and compliance information and facilitates the activities of licensing, policy, and compliance officers. The collection and storage of personally identifiable information (PII) is necessary for DDTC to ensure commercial exports of defense articles and defense services advance U.S. national security and foreign policy objectives. Lastly, DECCS supports the implementation of U.S. Government export controls of defense articles and defense services. The controls are imposed by the Arms Export Control Act (AECA) and the Department of State regulation that implements the AECA export controls - the International Traffic in Arms Regulations (ITAR).

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

PII is collected in DECCS for all registration and license applicants and for Advisory Opinions and Commodity Jurisdictions. In some cases, fields containing PII may not be required for all entities using DECCS. The data below are collected on U.S. citizens and non-U.S. persons unless otherwise specified. The following is a list of all PII collected by DDTC that is stored and processed in DECCS:

- Is the DECCS user a natural person or entity?
    - If person, name (first, middle, last)
    - If entity, company name
- Legal/Mailing/Place of Business/Place of Residence Address
    - Street Address
    - City
    - State/Province
    - Country
    - Zip/Postal Code
- Nationality
- Passport Number (non-US)
    - Country of Passport
    - Dual or Third-Country National (non-US)
- Visa Number (non-US)
- 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
- Points of Contact (POCs) of applicants
  - Name
  - Telephone
  - Email
  - Address
  - City
  - State/Province
  - Country
  - Zip/Postal Code

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

- Section 38 of the 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.
- 22 U.S.C. 2778(b)(1)(A)(i) authorizes DDTC to collect information from "every person…who engages in the business of manufacturing, exporting, or importing any defense articles or defense services" as those persons "shall register with the United States Government agency changed with the administration of this section.
- Section 40A of the AECA, 22 U.S.C. 2785, directs DDTC to establish an end-use monitoring program for export approved items.
- Though some authorities in the law are granted to the Department, and some to the President, all have been delegated to DDTC, either through Executive Order 13637, or through the regulations that implement the AECA, the ITAR, 22 C.F.R. Parts 120-130.

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

☒Yes, provide:

- SORN Name and Number: STATE-42 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 Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  N/A

- Disposition Authority Number:
  DAA-0059-2019-0012-0004

- Length of time the information is retained in the system:
  Temporary. Cut-off at the end of calendar year of final action. Destroy 25 year(s) after cutoff.

- Type of information retained in the system:
  Records documenting the registration of DECCS users [U.S. manufacturers and exporters of defense articles, defense services and all related technical data]. Records are arranged by case number, company, and country and includes, but are not limited to, application for registration, receipts for registration fees, correspondence, and related records.

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) On what other entities above is PII maintained in the system?

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other
☐ N/A

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

☐Yes ☐No ☒ N/A

- If yes, under what authorization?
  22 U.S.C. 2778, 2785 (AECA section 40A)

(d) How is the PII collected?

All PII is obtained directly from the DECCS user electronically through forms DSP-5, DSP-6, DSP-61, DSP-62, DSP-73, DSP-74, DSP-85, DS-2032, DS-4294, and DS-6004 that have been approved by the Office of Management and Budget (OMB). The information from the form is automatically uploaded into the system once the applicant pushes "submit". These forms are presented to the user via the DECCS web application transmitted using secure http (https) transport layer security (TLS). The forms are subject to the Paperwork Reduction Act and have been approved by OMB and assigned the OMB Control Numbers 1405-0002, 1405-0003, 1405-0013, 1405-0021, 1405-0023, 1405-0092, 1405-0142, and 1405-0173.

(e) 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.

DECCS data are maintained in the Microsoft Azure Government (MAG) Cloud and Service Now Government Community Cloud (GCC). Both the MAG and GCC are authorized to host data categorized at a high impact through the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB).

(f) What process is used to determine if the PII is accurate?

The information that is entered into DECCS is obtained directly from the DECCS user. DECCS service desk personnel review the entered information related to the creation of the DECCS user accounts in accordance with DDTC policy and procedures.

The entity or individual submitting information into DECCS is responsible for verifying the data accuracy. DDTC makes the final determinations on registration and license applications based on the data the DECCS user provides. If the DECCS user determines there are inaccuracies in the information that they entered in DECCS, there are amendment options for the Registration or Licensing application. In the case of other DECCS applications, the DECCS user would have to submit a new case.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Yes, the information is current. DECCS users directly enter this information into DECCS and are responsible for ensuring their/their entity's information in DECCS is correct and current. Changes to an individual or entity's registration or licensing information must be submitted to the DDTC service desk in accordance with the ITAR. The DDTC service desk personnel process tickets and address requested and approved changes following DDTC policy and procedures.

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

No, the system uses DECCS user-submitted information. These submissions only contain information provided by the DECCS user, which may sometimes come from commercial sources or publicly available information.

(i) How was the minimization of PII in the system considered?

Collection of PII within DECCS is limited to what is necessary to support DDTC business functions and interactions with DECCS Users.

5. Use of information

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

Information collected through DECCS is used:

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

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

Yes, the information is relevant to the purpose of DECCS and DECCS collects the minimum amount of PII necessary to perform the DDTC regulatory mission. The PII is only stored to enable the system to perform the functions that it was designed to do. No collateral uses exist for the information collected by the system.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

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

Methods for analyzing the data include individual analysis, group analysis, interoffice analysis, and interagency analysis to perform the functions listed in question 3c.

(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

(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

(d) If the system will use test data, will it include real PII?
☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal:

- Department of State (DOS)
    - 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 Economic and Business Affairs (EB)
    - Bureau of European and Eurasian Affairs (EUR)
    - Bureau of International Security and Nonproliferation (ISN)
    - Bureau of Near Eastern Affairs (NEA)
    - Bureau of Oceans and International Environmental and Scientific Affairs (OES)
    - Bureau of Political-Military Affairs (PM)
    - Bureau of South and Central Asian Affairs (SCA)
    - Representative for Afghanistan and Pakistan (SRAP)
    - Bureau of Western Hemisphere Affairs (WHA)
    - Office of the Inspector General (OIG)

- Office of the Legal Adviser (L)
- Office of the Coordinator for Cyber Issues (S/CCI)

External:

- Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)
- Department of Commerce (DOC)
  - Bureau of Industry and Security (BIS)
  - Export Administration (EA)
  - Security/Export Administration
- Department of Defense (DOD)
  - Defense Security Service (DSS)
  - Defense Technology Security Administration (DTSA)
  - Air Force Office of Special Investigations (AFOSI)
  - Army Criminal Investigation Command (CID)
  - Naval Criminal Investigative Service (NCIS)
  - Defense Criminal Investigative Services (DCIS)
  - Defense Intelligence Agency (DIA)
- Department of Energy (DOE)
  - National Nuclear Security Administration (NNSA)
- Department of Homeland Security (DHS)
  - 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)
- Office of Foreign Assets Control (OFAC), Other participating agencies of the Export Enforcement Coordination Center (E2C2)
- House Foreign Affairs Committee
- Senate Foreign Relations Committee

(b) What information will be shared?

Internal: DECCS case information to include all PII listed in paragraph 3(d) is shared with the internal bureaus and offices listed in 6(a).

External: The Department collaborates with the outside agencies contained in section 6(a) on the data elements from licensing, commodity jurisdiction, or law enforcement cases and shares all PII in paragraph 3(d).

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

Internal: DECCS case information is shared within the DOS offices listed in 6(a) for the purposes of consultation, review, and/or recommendations related to registration, licensing, commodity jurisdiction, or law enforcement activities.

External:

- CBP receives PII related to the Licensing and Registration applications to verify license and registration data against their records to determine if an entity is authorized to export or import defense articles.

- OFAC receives registration data to inform mergers and acquisitions.

- DDTC uses USXPORTS, a DoD system that is used by other agencies to adjudicate CJ and license authorization requests, and where the final determinations are issued. Agencies only have access to licensing case data and associated PII as described in 3(d) that they have received staffing request for. Below are the staffing agencies available within USXPORTS:

    - DHS
    - DoD/DTSA
    - DOC/BIS/EA
    - DOE/NNSA
    - NASA

- 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).

To other agencies as necessary for intelligence or law enforcement purposes as either required or allowed, depending on the agency, under the AECA (22 U.S.C. 2778(e)). Also, agencies may request information that might contain PII for other purposes on a case-by-case basis so long as the request conforms with the requirements of the Privacy Act, 5 U.S.C. 552a(b).

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

Internal: DDTC leverages the Department's implementation of Microsoft Office 365 for data sharing among internal parties.

External: Information is shared by secure transmission methods including TLS using secure file transfer protocol (sFTP) or through USXPORTS.

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

Internal: Internal users with a valid need-to-know are provided password protected access to DECCS or the data are shared via internal email using the Department's Office 365 system. DOS-O365 information is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved Office 365 Cloud.

External: Interagency sharing arrangements are in place that detail the handling of shared information. DDTC provides the data that are needed to perform statutory and regulatory functions. The agreed data sets are sent via sFTP for DTSA, CBP, and BIS. DTSA's USXPORTS system is password protected and access is granted based on need to know by DTSA. Encrypted email is used for specific staff members of Congress and other external users.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, an approved Privacy Act Statement (PAS) appears on the DECCS login page and again as a splash screen immediately upon login prior to accessing any application. This PAS provides the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

A PAS is on the login screen for DECCS and appears as a splash screen after a user logs in. The splash screen requires a user to "accept" the terms of the PAS or is otherwise logged out. An applicant's consent must be expressly given prior to accessing the application. However, failure to provide the information may result in the inability to receive the requested service.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

U.S. citizens and legal permanent residents may request access to their records or information by following the procedure described in the System of Records Notice, Munitions Control Records, STATE-42. Notice of these procedures is provided in the Privacy Act statement associated with the form utilized for the data collection. Further, all DECCS Users that have active accounts can access their information.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

If a DECCS user determines there are inaccuracies in the information that they submitted to DECCS, the DECCS user who wishes to gain access to or to amend their records should write to the Director, Office of Information Programs and Services, STATE-42.

DECCS users with active user accounts can correct their information by following the instructions on the DDTC website (https://pmddtc.state.gov) under the DECCS FAQs section.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The main DDTC website (https://pmddtc.state.gov) provides instructions on how to contact the service desk. DECCS users are guided to the Contact Us page from the DDTC website, where email and phone contacts are available for the DDTC Response Teams and the Service Desk. Additionally, the Privacy Act statement associated with the form utilized for the data collection cites SORN State-42 which provides notice of the procedures to correct information.

8. Security Controls

(a) How is all of the information in the system secured?

Information in DECCS is secured in accordance with the Federal Information Security Modernization Act (FISMA) 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 are required for a Federal Information Processing Standards (FIPS) 199 high impact system. Additional security controls were selected over the minimum baseline for a high 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.

For data at-rest, DECCS is leveraging MS Database as a Service which uses transparent data encryption (TDE) for all data stored in SQL databases. Azure storage and all associated storage accounts are encrypted by default within Azure.

Microsoft is responsible for managing all keys for encryption of Azure SQL databases, storage, and storage accounts.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

- DECCS Internal User: Accesses application to support/perform business processes and has access to all PII referenced in 3(d).
- DDTC Help Desk: Supports DDTC and industry information submitters via the help desk and responds to tickets. Access to DECCS PII is limited to entity or individual name, email address, and phone number.
- DDTC Security: Performs security engineering and operational tasks as directed by the DDTC ISSO. Configures network security mechanisms, antivirus mechanisms, and continuous monitoring tools. Monitors information system events. Access to a limited subset of DECCS PII may be necessary to support incident response efforts. This is restricted to entity or individual name, point of contact name, phone number, and email address.
- DDTC Administrator: Administers the cloud services, virtual servers, and migration of software updates / patches. No access to DECCS PII.
- Corporate Administrator (External DECCS Users): Manages the profile for their entity and grants access to other members of the organization. Submits documents necessary for registration, licensing. Access to all PII fields in 3(d) applicable to their own company only.
- Industry General (External DECCS Users): Views registration and licenses and associated status. Access is limited to PII associated with their own company only and based on assigned access from the corporate industry administrator.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Access control is implemented across DECCS based on the role of the individual who has an official need to access the information, 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 their job function and/or position. DECCS users are granted access to view only the information that they, themselves, submit. Access to other information related to their company is denied unless the company's point of contact grants the individual access to the company's information.

(d) How is access to data in the system determined for each role identified above?

- Internal DECCS Users: Internal DECCS users are granted access based on a service request where a supervisor submits an access request and a security team member reviews and approves or rejects the request based on the user's job duties. The DDTC ISSO grants access to security team members.
- External DECCS Users: External DECCS users must identify a corporate administrator that determines the role and access for members of their organization. This corporate administrator manages the DECCS user profile for their company and can assign access (if any) to other members of their organization, as they determine appropriate. The corporate administrator submits the documentation necessary for registration and licensing using the applicable forms in DECCS. DDTC only grants access to the External DECCS users' corporate administrator after the appropriate documentation is received in DECCS. DECCS users can only view their own PII.

(e) What monitoring, recording, auditing safeguards, and other controls 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. Within Sentinel and within Azure Alerts there are specific analytics policies that look for anomalies and privilege escalation as well as auditing log modification and/or attempts to delete data.

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.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no role-based training provided; however, DDTC personnel and contractors complete cyber security awareness training (Foreign Service Institute, PS800) that covers the procedures for handling Sensitive but Unclassified (SBU) information, including PII. Additionally, annual refresher training is mandatory, and records of successful completion are managed by IRM/CyberOps. DDTC personnel must also complete training for identifying and marking SBU information (Foreign Service Institute, PK400) and Protecting Personally Identifiable Information (Foreign Service Institute, PA318). These courses include instruction on how to properly identify and label sensitive information in electronic mail, IT systems and in paper. Refresher trainings are required every two years or annually, depending o