



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Financial and Air Clearance Transportation System (FACTS)

Department of the Navy - NAVSUP

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System New Electronic Collection
 Existing DoD Information System Existing Electronic Collection
 Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
 Yes, SIPRNET Enter SIPRNET Identification Number
 No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN Authorities:

Public Law 100-562, Imported Vehicle Safety Compliance Act of 1988
5 U.S.C. 5726, Storage Expenses, Household Goods and Personal Effects
10 U.S.C. 113, Secretary of Defense
10 U.S.C. 3013, Secretary of the Army
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 8013, Secretary of the Air Force, 19 U.S.C. 1498, Entry Under Regulations
37 U.S.C. 406, Travel and Transportation Allowances, Dependents, Baggage and Household Effects
Federal Acquisition Regulation (FAR)
Joint Federal Travel Regulation (JTR), Volumes I and II, DoD Directive 4500.9E, Transportation and Traffic Management; DoD Directive 5158.4, United States Transportation Command
DoD Instruction 4500.42, DoD Transportation Reservation and Ticketing Services
DoD Regulation 4140.1, DoD Materiel Management Regulation
DoD Regulation 4500.9, Defense Transportation Regulation
DoD Regulation 4515.13-R, Air Transportation Eligibility and E.O. 9397 (SSN),

Other Authorities:

5 U.S.C. 301, Departmental Regulations

10 U.S.C. 136 Under Secretary of Defense for Personnel Readiness
31 U.S.C. 3512(c) Executive Agency Accounting and Other Financial Management
50 U.S.C. Chapter 23, Internal Security
DoD Directive 1341.1, Defense Enrollment/Eligibility Reporting System
DoD Instruction 1341.2, DEERS Procedures
Homeland Security Presidential Directive 12, Policy for a common Identification Standard for Federal Employees and Contractors
38 CFR part 9.20

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The FACTS AIS application supports the clearance of all DoD air-eligible cargo for air shipment and facilitates Service first and second destination transportation funds management. FACTS provides shippers with Total Asset Visibility (TAV) of air-eligible cargo by furnishing cleared Advanced Transportation Control Movement Document (ATCMD) data to the Defense Transportation System (DTS), pre-obligation of transportation funds, and provides transportation billing validation and transportation budget forecasting for the Services. The FACTS AIS assists the shipper in determining Continental United States (CONUS) or Out of Continental United States (OCONUS) transportation mode routing selections by offering comparative mode, route, and cost information. FACTS AIS also plans and executes transport of vendor and Government shipments from the vendor's facility to the ultimate destination with 100% In Transit Visibility (ITV), standard and compliant documentation, at a cost favorable to the Government.

FACTS has established a secure electronic interface with the Defense Enrollment Eligibility Reporting System (DEERS). FACTS utilizes the data in this interface to validate personal property shipments flowing through the Defense Transportation System (DTS), thus authenticating eligibility of transportation related entitlements.

The data elements provided in this secure external interface include: Name, truncated, Social Security Number, Pay Grade/Rank, Service/Agency and Member Type (i.e., Military, Civilian).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The information obtained via the DEERS external interface is used by the FACTS application to authenticate eligibility of transportation related entitlements. This interface is secured via SFTP. The data at rest is encrypted, and access is limited to IT-1 Systems Administrators for database maintenance. The DEERS eligibility process is automated, and beyond the internal authentication of incoming personal property shipment information, there is no output of PII to FACTS reviewers and operators. Disclosure of information is granted only to those personnel using the FACTS application who maintain the tables and validate transportation related entitlements.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

NAVSUP. Information gathered is intended for use within the FACTS application and is not to be shared outside of the FACTS application.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

FACTS does not collect PII directly from the individual.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

[Empty rectangular box]

(2) If "No," state the reason why individuals cannot give or withhold their consent.

FACTS does not collect PII directly from the individual.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

FACTS does not collect PII directly from the individual.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.