

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Single Mobility System (SMS) Unclassified

2. DOD COMPONENT NAME:

United States Transportation Command

3. PIA APPROVAL DATE:

02/05/19

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
- From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

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

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

SMS is a suite of tools that provide for planning, visibility of requirements and missions (scheduled and unscheduled) and data visualization. SMS provides visibility of SAAM, Channel, OSA, contingency, exercise, Denton, Opportune, Guard, and Reserve missions and requirements. Additionally, it provides visibility of ship schedules, booked and manifested cargo, planning tools, port data and decision support tools such as port locators and station and ICAO workloads as well as mission monitoring of air, land, and sea conveyances. It provides visualization and analysis of JOPES data, exercise planning actions, force movement tracking, leading indicators for performance, executive management visualizations, tools for metrics and monitoring the state of the enterprise.

SMS receives PII via system interfaces; SMS receives PAX Manifest that contain name, rank and service. SMS may also receive Transportation Control Numbers (TCNs) from IGC that contain SSNs.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII received via systems is not used but rather embedded in the movement manifest and TCN which are used to track shipments. The other PII collected is required to verify the requester has a need for system access and to establish appropriate mission-related user privileges, but it is never uploaded into SMS.

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

For the PII that SMS receives via system interfaces, SMS has no contact (direct or indirect) with the individuals concerned. However, the originating systems provide the individual the opportunity to object to the collection of the PII.

For the PII that is needed to create user accounts, the user can not have an account created for them without supplying the requested PII, but it is never uploaded into SMS.

f. 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.

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

For the PII SMS receives via system interfaces, SMS has no contact (direct or indirect) with the individuals concerned. However, the originating systems provide the individual the opportunity to object to collection of the PII.

For the PII that is needed to create user accounts, the user can not have an account created for them without supplying the requested PII, but it is never uploaded into SMS.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

Privacy Act Statement Privacy Advisory Not Applicable

Privacy Act Statement:

For Foreign National

The Privacy Act of 1974, , 5 U.S.C. § 552a and applicable foreign law. This is directly taking from Single Mobility System Account Standard Operating Procedures.

"Note: personally identifiable information [PII] will be protected according to The Privacy Act of 1974, , 5 U.S.C. § 552a and applicable foreign law "

Privacy Advisory:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- | | | |
|--|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | All CCMDs |
| <input checked="" type="checkbox"/> Other DoD Components | Specify. | Military Services such as Navy, Army, Air Force, Marines |
| <input checked="" type="checkbox"/> Other Federal Agencies | Specify. | Federal Agencies such as FBI, DHS, and NSA |
| <input type="checkbox"/> State and Local Agencies | Specify. | |
| <input type="checkbox"/> Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) | Specify. | |
| <input type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | |

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- | | |
|---|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input checked="" type="checkbox"/> Other Federal Information Systems | |

From existing DoD system, i.e.. IGC, provided PII within system to system connection. The PII collected for account creation is sent via email to the SMS Account Managers and archived in the SMS Account Managers organization email. All emails are encrypted and digitally signed. The PII related to account creation is never uploaded into SMS.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- | | |
|---|--|
| <input checked="" type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

IGC provides PII within system to system connection. The PII collected for account creation is sent via email to the SMS Account Managers and archived in the SMS Account Managers organization email. All emails are encrypted and digitally signed. The PII related to account creation is never uploaded into SMS.

k. 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 must be consistent.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcld.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Disposition Authority	Date Signed by NARA	Disposition Comments	Authority	Date	Disposition
SMS-C CJCSM 5760.01 Vol 2	7/13/2012	System Documentation	N1-GRS-95-2 item 4, 7	4/1/2010	Data files, Input
SMS-U CJCSM 5760.01 Vol 2	7/13/2012	System Documentation	N1-GRS-95-2 item 4, 7	4/1/2010	Data files, Input

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

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 4140.1, DOD Supply Chain Material Management; DTR 4500.9-R, Defense Transportation Regulation; and DOD Instruction 4515.13, Air Transportation Eligibility and DOD Directive 4500.57, Transportation and Traffic Management.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Does not collect from Public