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:

Global Decision Support System (GDSS) - Unclassified (U)

2. DOD COMPONENT NAME:

United States Transportation Command

3. PIA APPROVAL DATE:

10/04/22

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees
- [ ] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

GDSS-Unclassified
GDSS is a National Security System (NSS) and the Mobility Air Force's primary command and control execution system residing on both the unclassified non-classified internet protocol router network (NIPRNet) and classified secure internet protocol router network (SIPRNet). GDSS automates the planning, management, and execution of airlift and air refueling missions for over 19,000 users at 261 worldwide locations. The primary focus of GDSS is to support U.S. Air Forces Europe-Air Forces Africa (USAFE), Pacific Air Forces (PACAF), and the 618th Air Operations Center (AOC) Tanker and Airlift Control Center (TACC) in mission planning and execution.

a. GDSS support includes flight management, which provides a completed crew mission package and files flight plans with Air Traffic Control (ATC) agencies.

b. GDSS contains aircrew member information, including the full Social Security Number (SSN) and utilizes individual user's 16-character DOD ID (Electronic Data Interchange Personnel Identifier (EDIPI)) for user account management for the lifetime of the account.

c. Critical to the mission planning and execution process is aircrew scheduling, which includes, but is not limited to aircrew management, qualification reviews, and flight authorizations. the GDSS user's account assigned location, unit, squadron and role-based access strictly controls individual GDSS user access to an aircrew members information. Role-based options include full-SSN view, last-4 of the SSN, or no SSN. A user's role is assigned and approved based on operational requirement needs.

d. GDSS utilizes individual user's EDIPI to manage an individual's role-based access to the GDSS system and linking to the user's Common Access Card (CAC) for authentication. Specifically, GDSS utilizes Personally Identifiable Information (PII) to: (1) Account for mission critical, military command, and control applications; (2) Manage aircrew member qualification and training; (3) Generate Aircrew Flight Authorization orders; and (4) Manage and authenticate user access to the GDSS systems and its applications.

e. GDSS does not share the full SSN with other interface partners (i.e., Air National Guard (ANG), Data and Web Services (DAWS), Distribution Component Billing System (DCBS), Air Mobility Command (AMC) Maintenance System (G081), Global Air Transportation Execution System (GATES), Mobility Enterprise Information System 4 (MEIS 4), and Single Mobility System (SMS)), although GDSS sends a truncated SSN (last 4 SSN) when sharing mission data outside of GDSS (i.e., the systems identified above).

The PII GDSS collects is a user's home and cell phone, mailing and home address, passport information, work e-mail address, marital status (in the form of spouse information), position and title, rank or grade, security information, DOD ID number, emergency contact, gender, name(s), and SSN.

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)*

Flying aircrew member SSNs (PII) originate from the Aviation Resource Management System (ARMS) and the GDSS Crew Management application for Mission Essential Personnel (MEPs), non-flying aircrew members. This information is required to facilitate the AMC (Air Mobility aircrew schedulers) management of training events and data, generation of Aircrew Flight Authorizations, and mission management in GDSS. These tasks include assigning aircrew and training, ensuring aircrew members the requisite qualifications and

training for missions, assigning aircrew members to missions, and generating Crew Flight Authorization orders. GDSS utilizes individual user's EDIPI to manage an individual's role-based access to the GDSS system and linking to the user's Common Access Card (CAC) for authentication. Specifically, GDSS utilizes Personally Identifiable Information (PII) to: (1) Account for mission critical, military command, and control applications; (2) Manage aircrew member qualification and training; (3) Generate Aircrew Flight Authorization orders; and (4) Manage and authenticate user access to the GDSS systems and its applications.

e. Do individuals have the opportunity to object to the collection of their PII? [X] 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.

The use of SSN is a required data element utilized to track and manage aircrew members; the user can contact ARMS and request that their crew records not be tracked by their SSN. When the source system (ARMS) migrates to utilizing another method of tracking aircrew members (e.g., EDIPI), GDSS will also convert and SSNs will no longer be required in the GDSS system. GDSS MEPs can object to having their SSN entered into GDSS; this could limit their ability to perform their flying duties as they could not be assigned to the mission or included within the Flight Authorizations. The use of the EDIPI is required for account creation and pairing with the user's Common Access Card (CAC) -- the user can refuse to provide their EDIPI; however, this would eliminate their ability to obtain a GDSS account.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

By signing the user account request, the user consents to the purpose of: "Provid[ing] positive identification of each individual requesting access."

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.)*

[X] Privacy Act Statement [X] Privacy Advisory [ ] Not Applicable

Privacy act statement reads as follows:
PRIVACY ACT STATEMENT
AUTHORITY: 10 U.S.C. 8013
PRINCIPAL PURPOSE: To apply for air travel. SSN is needed for positive ID.
ROUTINE US(S): Records from this system of records may be disclosed for any of the blanket routine uses published by the Air Force.
DISCLOSURE IS VOLUNTARY: Disclosure of SSN is voluntary; however, failure to provide the information may result in member not being accepted for travel on military aircraft.

PRIVACY ACT STATEMENT
AUTHORITY: 10 U.S.C. 8013
PRINCIPAL PURPOSE: Information is used to support a computer user account or an individual's system record.
Privacy Act of 1974 - AUTHORITY: 10 U.S.C. 8013, Secretary of the Air Force: powers and duties.
ROUTINE USES: The Department of the Air Force Blanket Routine Uses, published at the beginning of the Agency's compilation of record system notices, apply to this system. Disclosure is voluntary.

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

[X] Within the DoD Component	Specify.	Air Mobility Command - AMC U.S. Transportation Command - USTRANSCOM
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Department of Defense - DOD U.S. Army - USA U.S. Air Force - USAF U.S. Marine Corps - USMC U.S. Navy - USN
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	U.S. Coast Guard - USCG
[ ] State and Local Agencies	Specify.	

[X] 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. DTSI, eVETS, MITRE, OBXtek, Tapestry Solutions, and TRI-COR.
The contractor shall comply with Federal Information Processing Standards (FIPS) and Federal laws and regulations that affect IT systems operations.
Examples are the Privacy Act of 1974, the Computer Security Act of 1987, and the Joint Financial Management Improvement Program (JFMIP).

[ ] 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)*

[X] Individuals
[X] Existing DoD Information Systems
[X] Other Federal Information Systems
[X] Databases
[ ] Commercial Systems

ARMS, GDSS, ANG, DAWS, DCBS, G081, GATES, MEIS 4, and SMS, although GDSS sends a truncated SSN (last 4 SSN) when sharing mission data outside of GDSS to these systems.

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

[X] E-mail
[X] In-Person Contact
[ ] Fax
[X] Information Sharing - System to System
[ ] Other *(If Other, enter the information in the box below)*
[ ] Official Form (*Enter Form Number(s) in the box below)*
[ ] Paper
[ ] Telephone Interview
[ ] Website/E-Form

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier FTRANSCOM 01 DOD

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. DAA-GRS-2013-0006-0003

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

(3) Retention Instructions.

(1) Systems not requiring special accountability for access: Temporary. Destroy when business use ceases.
2) Systems requiring special accountability for access: Temporary. Destroy seven years after user account is terminated, but longer retention is authorized if required for business use.
NOTE: GDSS mission records are purged after 20 years from execution.

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 statue 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.

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; E.O. 9397 (SSN); DOD Instruction 4140.1, DOD Supply Chain Material Management; DOD Directive 4500.9E, Transportation and Traffic Management; DTR 4500.9-R, Defense Transportation Regulation; DOD Directive 4500.57, Transportation and Traffic Management; DOD Instruction 4515.13, Air Transportation Eligibility and DOD Directive 5158.4, U.S. Transportation Command.

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.

DOD Manual 8910.01, Volume 2 does not apply to DOD internal information collections that do not collect information from members of the public.