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:

Cargo Movement Operations System

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

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
- [x] 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
- [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.

CMOS provides the capability to effectively plan, document, and manage outbound and inbound cargo and to plan, schedule, and monitor the execution of transportation activities in support of deployment and reception of forces. The system accumulates and aggregates shipment data, tracks the completion of transportation actions, prepares and prints movement documentation, prepares and transmits advance shipment notification to all involved activities, and prepares and transmits system reports. System records are used to determine passenger movement trends and prepare aircraft manifests.
Information collected includes full name, personal identification (Social Security Number (SSN), or DoDID (EDIPI), or passport number), grade, travel order, transportation authorizations, seats required, origin, destination, requested travel dates, routing indicator (identifies the activity/installation requesting the reservation), cancellation and standby codes (identifies the reason the passenger did not depart as scheduled), flight number, departure date and reporting time, and administrative coding (such as a Leave Form number) as appropriate.

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)*

Authentication and validation of passenger identity for movement on military and commercial aircraft.

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

Per Defense Transportation Regulation Part 1, Chapter 103 (A 6c (17), Passenger Movement (22 February 2017), the following personal information is mandatory: DoDID or Social Security Number (SSN); Rank; Service Code Army (A), Air Force (AF), Navy (N), Marine Corps (MC), Coast Guard (CG), Civilian (CIV); Last Name; First Name; Middle Initial; Gender Male (M) or Female (F); The name and telephone number of an emergency contact not traveling with the passenger.
Document can be obtained from the following URL: https://www.ustranscom.mil/dtr/part-i/dtr_part_i_103.pdf.

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

Per Defense Transportation Regulation Part 1, Chapter 103 (A 6c (17), Passenger Movement (22 February 2017), the following personal information is mandatory: DoDID or Social Security Number (SSN); Rank; Service Code Army (A), Air Force (AF), Navy (N), Marine Corps (MC), Coast Guard (CG), Civilian (CIV); Last Name; First Name; Middle Initial; Gender Male (M) or Female (F); The name and telephone number of an emergency contact not traveling with the passenger.
Document can be obtained from the following URL: https://www.ustranscom.mil/dtr/part-i/dtr_part_i_103.pdf

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

Authority: 10 U.S.C. 8013, Secretary of the Air Force; DoD 4500.9R, Defense Transportation Regulation; Air Force Program Management Directive #5272(2)/38610F, Cargo Movement Operations System; and E.O. 9397 (SSN), as amended.
Purpose: Data is collected to authenticate and manifest personnel moving within the Defense Transportation Network
Routine Uses: This information is electronically transmitted to the Global Air Transportation Execution System (GATES) and Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence (IGC) for manifest management. In the case of an incident such as a crash, the manifest is given to the Federal Aviation Administration (FAA) for notification of the listed passenger emergency contacts.
Disclosure: Mandatory; Failure to provide the required information will result in the passenger not being allowed on the flight.

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

☐ Within the DoD Component	Specify.	
☐ Other DoD Components	Specify.	
☒ Other Federal Agencies	Specify.	To other Federal agencies and offices to provide passenger manifest information. To Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence (IGC) to use the data for the purpose to manifest passengers on military and government civilian contracted aircraft. The DoD ‘‘Blanket Routine Uses’’ published at the beginning of the Air Force’s compilation of systems of records notices apply to this system.
☐ State and Local Agencies	Specify.	
☐ 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.	
☐ 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)*

☒ Individuals ☐ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☐ Other Federal Information Systems

The PII is collected from existing DoD information System (Deliberate Crisis Action Planning and Execution Segments - DCAPES) and used to manifest passengers on military and commercial aircraft.

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

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*
☒ Face-to-Face Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☒ Information Sharing - System to System ☐ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

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 F024 AF AFMC A

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.

Retained IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedules:
T 24 - 01 R 03.00 T 24 - 01 R 04.00 T 24 - 01 R 09.00 T 24 - 01 R 10.00 T 24 - 02 R 01.00

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.

DoD/AF privacy laws, regulations, or mandates apply. 10 U.S.C. 8013, Secretary of the Air Force; DoD 4500.9R, Defense Transportation Regulation; Air Force Program Management Directive #5272(2)/38610F, Cargo Movement Operations System; and E.O. 9397 (SSN), as amended.

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.

CMOS is a DoD joint-use, AF-managed combat support system and is not a public information collection system.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☐ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☒ Emergency Contact
☐ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☐ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☐ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☐ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☒ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

RICHARD T. ALDRIDGE, SES, DAF
Program Executive Officer
Signature date 08-AUG-2018

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

In accordance with DTM 07-015-USD (P&R), DoD Social Security Number (SSN) Reduction Plan, CMOS is justified under the SSN Use Case category "Computer Matching". CMOS shares manifest information, which may include SSN data, with:
• Global Air Transportation Execution System (GATES)
• Integrated Data Environment (IDE)/Global Transportation Network (GTN) Convergence (IGC)

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

The SSN data input field has been relabeled as "ID."
Individuals have the option of providing a passport or DoDID (EDIPI) number in lieu of SSN.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☒ Yes ☐ No

Mitigation efforts have already been implemented. In support of that, the data input field has been relabeled as "ID." When all passengers use either an EDIPI or Passport number, SSN entry will no longer be needed, though the data will remain resident in CMOS or its successor system for 7 years due to existing documentation retention requirements.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [x] Combination Locks
- [ ] Key Cards
- [ ] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [ ] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

Locked rooms and cabinets as well as masked in the system and printed products for all but last four digits.

(2) Administrative Controls. *(Check all that apply)*

- [x] Backups Secured Off-site
- [ ] Encryption of Backups
- [ ] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [ ] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [ ] Encryption of Data at Rest
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Command Access Card (CAC)
- [x] Encryption of Data in Transit
- [ ] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [ ] Least Privilege Access
- [ ] User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Records are accessed by person(s) responsible for servicing the record system in performance of their official duties and by authorized personnel who are properly screened and cleared for need-to-know. Records are stored in locked rooms and cabinets. Those in computer storage devices are protected by computer system software.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	451
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[ ]	Yes, RMF tool	RMF tool Identification Number	
[ ]	No		

If “No,” explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, “Risk Management Framework for DoD Information Technology”.

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	10/18/2017
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

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

[X] Yes [ ] No

If "Yes," Enter UII 007-57-01-03-01-0317-00 If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Johnnie E. Mize	(1) Title	Program Manager, CMOS
(2) Organization	AFMC AFLCMC/HIAR	(3) Work Telephone	334-416-4616
(4) DSN	596-4616	(5) E-mail address	johnnie.mize@us.af.mil
(6) Date of Review	08/21/19	(7) Signature	MIZE.JOHNNIE.E.JR.1104851416 Digitally signed by MIZE.JOHNNIE.E.JR.1104851416 Date: 2019.08.21 15:58:03 -05'00'
b. Other Official *(to be used at Component discretion)*	Richard A. Swezey	(1) Title	Chief, AF Cargo Policy
(2) Organization	HAF/A4LR	(3) Work Telephone	703-697-8137
(4) DSN	312-227-8137	(5) E-mail address	richard.a.swezey.civ@mail.mil
(6) Date of Review	8/22/1019	(7) Signature	SWEZEY.RICHARD.ALAN.1175720878 Digitally signed by SWEZEY.RICHARD.ALAN.1175720878 Date: 2019.08.22 10:20:16 -04'00'
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

e. Component Records Officer		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
f. Component Senior Information Security Officer or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review:		(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.