

BILLING CODE:

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2021-DMDC - XXXX]

Privacy Act of 1974; System of Records

AGENCY: Defense Manpower Data Center

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is modifying and reissuing a current system of records titled, Non-Combatant Tracking System (NTS) & Evacuation Tracking System (ETAS) DMDC 04. This system of records was originally established by the Defense Manpower Data Center (DMDC) to collect and maintain records on the tracking and accountability for individuals evacuated from emergency situations due to military operations, political situations, natural disasters, or other potentially dangerous circumstances.

***This system of records notice (SORN) is being updated to...**

Repatriations centers will use this information to track and account for individuals evacuated from emergency situations and assist in security requested relocation and assistance services, and recording and recovering relocation costs. ETAS units will collect information to triage or manage a large number of personnel in CONUS-based situations. The types of personal information being collected on individuals include:

Evacuee: registration location and date, Country Evacuated From, Location Code (e.g., airport, ship port), removal location and date, person ID (passport number, social security number, foreign ID number, U.S. driver's license number, electronic data interchange number), person ID document expiration date, evacuee ID (bracelet, triage tag, other ID), DHS traveler number, DHS redress number, name, date of birth, sex, marital status, familial relation, sponsor Information email address, phone number, country of citizenship, country of residence, DoD affiliation, final destination (city, state, country), evacuee minor category (i.e., pregnant/trimester, unaccompanied child, aged and infirm)

Medical Flag, Mobility, Triage Category & Information, Transportation Information and identification of any Special Needs (e.g., oxygen, wheelchair, food allergy) evacuee minor category (i.e., pregnant/trimester, unaccompanied child, aged and infirm), medical patient (Y/N), mobility (ambulatory, non-ambulatory, deceased), triage category, special needs (e.g., oxygen, wheelchair, food allergy,

Evacuee Contact: name, email address, phone number, country of residence,

Evacuee Sponsor: name, date of birth, sex, relationship to evacuee, service branch, personnel category, unit identification code

Evacuee Pet: name, type, bracelet, microchip

Manifest: departure location (city, country, ICAO/MILAIR/MILSEA code), transportation vehicle (type, identification, departure date/time), destination location (city, country, ICAO/MILAIR/MILSEA code), arrival date/time, passenger list with date/time added and arrived, mission ID

Users: Name, electronic data interchange number, location and date of registration

Unit ID number, classification number, agency code (identifying DoD or other U.S. Federal Agency sponsorship), service branch, title/rank, personnel category,

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by either of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: The Defense Manpower Data Center, Privacy Office, DoD Center Monterey Bay, 400 Gigling Road, Monterey, CA 93955, or by Email: dodhra.dodc-mb.dmdc.mbx.webmaster@mail.mil

SUPPLEMENTARY INFORMATION:

I. Background

The Non-Combatant Tracking System (NTS) & Evacuation Tracking System (ETAS) is used to track and account for individuals evacuated from emergency situations and assist in requested relocation and assistance services, and recording and recovering relocation costs.

Subject to public comment, the Department of Defense (DoD) proposes to update this system of records to add the standard DoD routine uses (routine uses A through I) subject to the Privacy Act of 1974, 5 U.S.C. 552a.

Additionally, the following sections of the SORN system of records notice (SORN) is being modified as follows to...

DoD SORNs have been published in the Federal Register and are available through the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.defense.gov/privacy>.

II. Privacy Act

Under the Privacy Act, a “system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, Defense Privacy and Civil Liberties and Transparency Division (DLPTD) has provided a report of this system of records to the Office of Management and Budget (OMB) and to Congress.

Dated:

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: NON-COMBATANT TRACKING SYSTEM (NTS) &
EVACUATION TRACKING SYSTEM (ETAS) DMDC 04

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Defense Manpower Data Center, DoD Center Oracle Cloud
Environment Ashburn, VA ,

SYSTEM MANAGER(S): The system manager is: Malcolm Mejia Program Manager,
Defense Manpower Data Center, 400 GIGLING ROAD. SEASIDE, CA 93955-6771.
Email: dodhra.dodc-mb.dmdc.mbx.webmaster@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

E.O. 12656, Assignment of Emergency Preparedness Responsibilities, as amended; E.O.
9397 (SSN), as amended, J.P. 3-68 Noncombatant Evacuation Operations, and DoDD
3025.14 Evacuation of U.S. Citizens and Designated Aliens from Threatened Areas
Abroad.

PURPOSE(S) OF THE SYSTEM: Repatriation centers will use this information to track and account for individuals evacuated from emergency situations due to military operations, political situations, natural disasters, or other potentially dangerous circumstances. Repatriation centers assist evacuees in securing requested relocation services, and recording and recovering relocation costs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Service members and their dependents, DoD and other federal civilian employees and their dependents, U.S. Government contractors, U.S. citizens, foreign nationals working for the U.S. government and foreign nationals evacuated to the U.S., or OCONUS Safehavens.

CATEGORIES OF RECORDS IN THE SYSTEM:

Evacuee: registration location and date, Country Evacuated From, Location Code (e.g., airport, ship port), removal location and date, person ID (passport number, social security number, foreign ID number, U.S. driver's license number, electronic data interchange number), person ID document expiration date, evacuee ID (bracelet, triage tag, other ID), DHS traveler number, DHS redress number, name, date of birth, sex, marital status, familial relation, sponsor Information email address, phone number, country of citizenship, country of residence, DoD affiliation, final destination (city, state, country), evacuee minor category (i.e., pregnant/trimester, unaccompanied child, aged and infirm)

Medical Flag, Mobility, Triage Category & Information, Transportation Information and identification of any Special Needs (e.g., oxygen, wheelchair, food allergy) evacuee minor category (i.e., pregnant/trimester, unaccompanied child, aged and infirm), medical patient

(Y/N), mobility (ambulatory, non-ambulatory, deceased), triage category, special needs (e.g., oxygen, wheelchair, food allergy,

Evacuee Contact: name, email address, phone number, country of residence,

Evacuee Sponsor: name, date of birth, sex, relationship to evacuee, service branch, personnel category, unit identification code

Evacuee Pet: name, type, bracelet, microchip

Manifest: departure location (city, country, ICAO/MILAIR/MILSEA code), transportation vehicle (type, identification, departure date/time), destination location (city, country,

ICAO/MILAIR/MILSEA code), arrival date/time, passenger list with date/time added and arrived, mission ID

Users: Name, electronic data interchange number, location and date of registration

UNIT ID NUMBER, CLASSIFICATION NUMBER, AGENCY CODE (IDENTIFYING DOD OR OTHER U.S. FEDERAL AGENCY SPONSORSHIP), SERVICE BRANCH, TITLE/RANK, PERSONNEL CATEGORY,

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: Disclosure by the person in the form, of providing passports, government issued ID cards, Common Access Cards, and U.S. driver's licenses, and interviews with the individual.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended,

all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. To individuals who have been evacuated but who have been separated from their family and/or spouse. Information will be released to the individual indicating where the family member was evacuated from and final destination.

K. To Department of State to plan and monitor evacuation effectiveness and need for services and to verify the number of people by category who have been evacuated.

L. To the Transportation Command (TRANSCOM), Global Air Transportation Execution System (GATES) for use of manifest and evacuee data to reduce duplication of effort to record this information.

M. To DoD Common Operational Picture (COP) systems like Combined Information Data Network Exchange (CIDNE), Situational Awareness Geospatial Enterprise (SAGE) and Advanced Analytics (ADVANA) for stakeholder views of evacuation resources and progress.

N. To the Department of Homeland Security (DHS) router to meeting requirement to vet incoming passengers to the U.S. against systems like Advance Passenger Information System (APIS) to check against the do not fly list.

O. To the American Red Cross so that upon receipt of information from a repatriation center that a DoD family has arrived safely in the U.S., the Red Cross may notify the service member (sponsor) still in the foreign country that his/her family has safely arrived in the United States.

P. To the U.S. Citizenship and Immigration Service to track and make contact with all foreign nationals who have been evacuated to the U.S.

Q. To the Department of Health and Human Services to facilitate the delivery of personal and financial assistance and to recoup the costs of financial services. To identify individuals who might arrive with an illness which would require quarantine.

R. To the Internal Revenue Service to recoup unpaid loans made on an emergency basis as a result of emergency evacuation.

S. To State and local health departments to further implement the quarantine of an ill individual.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud

environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by ID Number and type, name, and evacuee ID which include EDI, Driver's License Number, Passport Number, or SSN.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained for: Permanent: Cut off (take a snapshot) at end of fiscal year and transfer to the National Archives and Record Administration in accordance with 36 CFR 1228.270 and 36 CFR 1234.

ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS: The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; Secret Internet Protocol Router (SIPR) token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical

access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; Secret Internet Protocol Router (SIPR) token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the Deputy Director, Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

Individuals should provide the following:

- a. Full name, former name, and any other names used.
- b. Date and place of birth.
- c. Social Security Number.
- d. The address to which the record information should be sent.
- e. The name and number of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside of the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).'

If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).'

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf. The written authorization must also include an original notarized statement or an unsworn declaration in accordance with 28 U.S.C. 1746, in the following format:

I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, for contesting contents and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the above instructions for “Record Access Procedures”.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY:

April 15, 2016, 81 FR 22242; April 14, 2009, 74 FR 17173