BY ORDER OF THE COMMANDER
UNITED STATES TRANSPORTATION COMMAND

USTRANSCOM INSTRUCTION 33-35
18 NOVEMBER 2014

Communications and Information

PRIVACY ACT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available electronically on the USTRANSCOM electronic library.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: TCJA-FO
Approved By: TCJA (Colonel Michael J. Benjamin USA)
Supersedes: USTRANSCOMI 33-35, 20 October 2003
Pages: 26
Distribution: e-Publishing

This instruction establishes policies, procedures, and responsibilities for implementing the United States Transportation Command (USTRANSCOM) Privacy Act (PA) Program governing collecting, safeguarding, maintaining, using, accessing, amending, and disseminating personal information maintained by USTRANSCOM systems of records. This instruction is applicable to all personnel assigned to USTRANSCOM. The components will follow their Service instructions for information maintained by systems of records generated within their area of responsibility. This instruction implements Federal law, Department of Defense (DOD), and Air Force (AF) regulations listed in Attachment 1, and contains additional instructions and guidance affecting the USTRANSCOM Privacy Act Program. Use in conjunction with those publications. This instruction does not apply to Freedom of Information Act (FOIA) requests, information from systems of records controlled by the Office of Personnel Management (although maintained by a DOD component), or requests for personal information from the General Accounting Office. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10 United States Code Section 8013. System of Records Notice F033 AF B, Privacy Act Request File, applies. Maintain and dispose of records created as a result of processes prescribed by this instruction in accordance with Chairman Joint Chiefs of Staff Manual (CJCSM) 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule. A USTRANSCOM member can file a civil suit against their respective Service for failure to comply with the Privacy Act; for example, willfully maintaining a system of records that doesn't meet the public notice requirements; disclosing information from a system of records to someone not entitled to the information, or obtaining records under false pretenses. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

SUMMARY OF REVISIONS

This instructions was revised for realignment under the Staff Judge Advocate

1. REFERENCES AND SUPPORTING INFORMATION. References, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. POLICY. The Privacy Act of 1974 and this instruction apply to information contained in USTRANSCOM Privacy Act systems of records.

2.1. An official system of records is authorized by law or Executive Order and required to carry out a USTRANSCOM mission or function.

2.2. USTRANSCOM does not:

2.2.1. Keep records on how a person exercises First Amendment rights. *Exceptions* are when USTRANSCOM has the permission of that individual or are authorized by federal statute, or the information pertains to an authorized law enforcement activity.

2.2.2. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act and will give reasonable aid to individuals exercising their rights.

2.3. USTRANSCOM staff members will:

2.3.1. Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems of records published in the Federal Register.

2.3.2. Collect, maintain, and use information in such systems only to support programs authorized by law or Executive Order.

2.3.3. Safeguard records included in the systems and keep them the minimum time required.

2.3.4. Keep the records timely, accurate, complete, and relevant.

2.3.5. Amend and correct records on request.

2.3.6. Let individuals review and receive copies of their own records unless an exemption for the system exists or records were created in anticipation of a civil action or proceeding.

2.3.7. Provide a review of decisions that deny individuals access to or amendment of their records.

2.4. Personal Notes. The Privacy Act does not apply to personal notes on individuals for use as memory aids to supervise or perform other official functions that are not shared with others and no USTRANSCOM directive requires maintenance.

2.5. Systems of Records Operated By a Contractor. Contractors who are required to operate or maintain a Privacy Act system of records by contract are considered employees of USTRANSCOM during the performance of the contract. The record system affected is maintained by USTRANSCOM and is subject to this instruction. Offices that have contractors operating or maintaining such record systems must ensure the contract contains the proper Privacy Act clauses, and identify the record system number. Records maintained by the contractor for the management of contractor employees are not subject to the Privacy Act.

3. RESPONSIBILITIES.

3.1. Chief, TCJA-FO will serve as the USTRANSCOM Privacy Act Officer. The Privacy Act Officer will manage the program; guide and train; review the program at regular intervals; review all publications and forms for compliance with this instruction; review proposed new, altered, and amended systems notices; review/resolve complaints or allegations of Privacy Act violations; review annually contracts for systems of records operated or maintained by a contractor; answer general Privacy Act questions and correspondence; and staff denial recommendations.

3.2. Systems of Records Managers are the officials who are responsible for managing a system of records, including policies and procedures to operate and safeguard it. Systems Managers will decide the need for and content of systems; manage and safeguard the system; train personnel on PA requirements; protect records from unauthorized disclosure, alteration, or destruction; prepare systems notices and reports; answer Privacy Act requests; investigate complaints or allegations, establish and review the facts, interview individuals as needed, determine validity of the complaint, and take appropriate corrective action; keep records of disclosures; and evaluate the systems annually.

3.3. Service Element Commanders, Directors, Command Support Group (CSG) Chiefs, Functional Managers, and Supervisors within USTRANSCOM are responsible for ensuring Privacy Act data under their control comply with the following:

3.3.1. USTRANSCOM Force Protection (TCJ3-FP) may request information from other agencies for law enforcement purposes under Title 5 United States Code Section 552a (b) (7). TCJ3-FP must indicate in writing the specific part of the record desired and identify the law enforcement activity requesting the record.

3.3.2. Record promises of confidentiality to exempt from disclosure any "confidential" information under Title 5 United States Code 552a, Subsection (k)(2), (k)(5), or (k)(7) of the Privacy Act.

3.3.3. Collect personal information directly from the subject of the record when possible. Third parties may be asked when information must be verified, opinions or evaluations are required, the subject cannot be contacted, or the subject requests the information be obtained from another person.

3.3.4. Give a Privacy Act Statement (PAS) orally or in writing to anyone from whom personal information is collected for a system of records, and whenever an individual's Social Security Number is requested. *(NOTE: Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked; however, does not ask the person to sign the PAS.)* A PAS must include the following four items: (See Attachment 2 for sample PAS.)

3.3.4.1. Authority: The legal authority is the United States Code or Executive Order authorizing the program the system supports.

3.3.4.2. Purpose: The reason the information is collected.

3.3.4.3. Routine Uses: A list of where and why the information will be disclosed outside DOD.

3.3.4.4. Disclosure: Voluntary or Mandatory. Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information. Include any consequences of nondisclosure in nonthreatening language.

3.3.5. Social Security Numbers (SSN).

3.3.5.1. Disclosure. Do not disclose an individual's Social Security Number (SSN) without an official need to know, this includes disclosing to personnel in USTRANSCOM and DOD-wide. Outside the DOD, SSN is not releasable under the DOD Privacy Act Program without the individual's consent, unless authorized under 1 of the 12 exceptions to the "No Disclosure Without Consent" Rule (DOD 5400.11-R, Privacy Program).

3.3.5.2. Reduction of SSN Use in DoD.

3.3.5.3. Responsibility.

3.3.5.3.1. Provide the final approval authority for SSN use and justification. The authorization for use of PII is governed through the DoD Privacy Program in accordance with References (j) and (k).

3.3.5.3.2. Review SSN use and justifications in the DITPR, in accordance with the guidance in Reference (m), as part of the biennial Privacy Act SORN review, required by the Defense Privacy Program, and prepare an annual report on results as described in Enclosure 3.

3.3.5.3.3. Submit the annual report required by section 3544(c) of Reference (l). This report requires agencies to review and update their progress on the reduction of holdings of PII. Provide specific guidance annually to reflect the reporting elements. FISMA elements are subject to change. The DoD Component Privacy offices are responsible for providing input to the DPCLO for inclusion in the report.

3.3.5.3.4. Established detailed guidance and additional reports as necessary to support DOD efforts in SSN collection, use dissemination, and reduction.

3.3.6. Medical Information. Service element commanders, directors, CSG chiefs, functional managers, and supervisors within USTRANSCOM, where appropriate, are responsible for ensuring that the handling and release of protected healthcare information are in accordance with DOD 6025.18-R, DOD Health Information Policy Regulation.

4. DENIAL AUTHORITIES. The USTRANSCOM Staff Judge Advocate (TCJA), and in his/her absence the Deputy Staff Judge Advocate (TCJA-D) are the USTRANSCOM Privacy Act denial authorities. Access denials are processed within five workdays from receipt of the request for access. The System Manager for the information requested will prepare the

"Recommendation for Access Denial" package to include a copy of the request, the record requested, and applicable exemption. TCJA-FO will coordinate proposed denials with the command denial authority (TCJA or TCJA-D). Notification of denials to requesters will include statutory authority, reason, and pertinent appeal rights. Ensure the system has an approved exemption published as a final rule in the Federal Register; the exemption covers each document (all parts of a system are not automatically exempt); and nonexempt parts are segregated before denying access to a record.

4.1. Medical Records. If a physician believes that disclosing requested medical records could harm the person's mental or physical health, ask the requester to get a letter from a physician to whom you can send the records and include a letter explaining that giving the records directly to the requester could be harmful. If naming a physician poses a hardship, offer the services of military physician other than the one who provided treatment; however, the requester is entitled to receive their records.

4.2. Third Party Information. Normally, when information in a requester's record is "about" or "pertains to" a third party, it is not considered the requester's record and should not be released. This is not considered a denial. However, if the requester will be denied a right, privilege, or benefit, the requester must be given access to relevant portions. If nonjudicial punishment or loss of privileges is the issue, appropriate portions will not be protected and will be released.

4.3. Civil Action Information. Records compiled in connection with a civil action or other proceeding, including any action where USTRANSCOM expects judicial or administrative adjudicatory proceedings will not be released. This exemption does not include criminal actions. Attorney work products prepared before, during, or after the action or proceeding will not be released.

5. REQUESTING ACCESS TO PRIVACY ACT RECORDS. USTRANSCOM members or their designated representatives may request a copy of their records in a system of records. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How identity is verified will depend on the sensitivity of the requested record. A request from an individual for his or her own records in a system of records will be considered under both the Freedom of Information Act (FOIA) and Privacy Act regardless of the Act cited; however, there is no requirement to cite either Act if the records they want are contained in a system of records. Process the request under whichever Act gives the most information. Requesters should describe the records they want, with at least a type of record or functional area if they do not have the system of records number. For "all records about me" requests, refer the requester to www.defenselink.mil/privacy/notices to review Systems of Records published in the Federal Register. Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making Privacy Act requests. If records exist, inform the requester how to review the record. If possible, respond to Privacy Act requests within 10 workdays of receipt, or send a letter explaining why the request cannot be responded to within 10 workdays and give an approximate completion date no more than 20 workdays. Requester should be shown or given a copy of the record within 30 workdays unless the system is exempt (see Paragraph 12). If the system is exempt provide any parts releasable under FOIA, with appeal rights, citing appropriate exemptions from the Privacy

Act and FOIA. If the requester wants another person present during the records review, the system manager may ask for written consent to authorize discussing the record with another person present. Give the first 100 pages free and charge only reproduction costs for the remainder at $.15 per page. Do not charge fees when the requester can get the record without charge under another publication, for search, for reproducing a document for the convenience of the command, or for reproducing a record so the requester can review it.

6. AMENDING THE RECORD.

6.1. Individuals may ask to have their records amended to make them accurate, timely, relevant, or complete. Systems managers routinely correct a record if the requester can show that it is factually wrong. Anyone may request minor corrections orally. Requests for more significant modifications should be in writing. After verifying the identity of the requester, make the change, notify all known recipients of the record, and inform the individual. Acknowledge requests for amendment within 10 workdays of receipt. Give an expected completion date unless the change is completed within that time. Final decisions must take no longer than 30 workdays.

6.2. USTRANSCOM will not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This action constitutes a denial, and requesters may appeal. If the system manager decides not to amend or partially amend the record, send a copy of the request, the record, and the recommended denial reasons to TCJA-FO who will coordinate with the command denial authority TCJA or TCJA-D. If the denial authority approves the request, amend the record and notify all previous recipients that it has been changed. Denial notification to requesters will include the statutory authority, reason, and pertinent appeal rights.

6.3. Requesters should pursue record corrections of subjective matters and opinions through proper channels to the 375th Civilian Personnel Section (FSMC) using grievance procedures or the specific Service Board for Correction of Military Records. Record correction requests denied by FSMC or Service Board for Correction of Military Records are not subject to further consideration under this instruction.

7. APPEAL PROCEDURES. Individuals may request a denial review within 60 calendar days after receiving a denial letter. The command Privacy Act Officer will complete the appeal package to include the original appeal letter, the initial request, the initial denial, a copy of the record, any internal records or coordination actions relating to the denial, denial authority comments on the appellant's arguments, and legal reviews, if applicable, and forward to Defense Privacy and Civil Liberties (DPCLO), 241 18th Street South, Suite 101, Arlington VA 22202. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately.

8. PRIVACY ACT NOTIFICATIONS.

8.1. USTRANSCOM will include a Privacy Act Warning Statement in each USTRANSCOM publication that requires collecting or keeping personal information in a system of records. Also

include the warning statement when publications direct collection of SSN from individuals. The warning statement will cite legal authority and the system of records number and title. You can use the following warning statement: "This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by (United States Code citation and or Executive Order number). System of Records Notice (number and title) applies."

8.2. Information systems that contain information on individuals that is retrieved by name or personal identifier are subject to the Privacy Act. These systems are required to have a Privacy Act system notice published in the Federal Register that covers the information collection. In addition, all information systems subject to the Privacy Act will have warning banners displayed on the first screen (at a minimum) to assist in safeguarding the information. Use the following: **"***PRIVACY ACT INFORMATION – The information accessed through this system is FOR OFFICIAL USE ONLY and must be protected in accordance with the Privacy Act and USTRANSCOM Instruction 33-35."*

8.3. Exercise caution before transmitting personal information over electronic mail (e-mail) to ensure it is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the proper way to transmit it. When sending personal information over e-mail within USTRANSCOM/DOD, ensure there is an official need; all addressees, including "cc" addressees, are authorized to receive it under the Privacy Act; and it is protected from unauthorized disclosure, loss, or alteration. Protection methods may include encryption or password protecting the information. When transmitting personal information over e-mail, add "FOUO" to the beginning of the subject line, followed by the subject, and the following statement at the beginning of the e-mail (do not apply to bottom of e-mails): *"This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Privacy Act and USTRANSCOMI 33-35."*

9. PRIVACY IMPACT ASSESSMENTS. The Electronic Government (E-Government) Act of 2002 requires a Privacy Impact Assessment (PIA) be conducted before developing or procuring information technology or initiating a new collection of information using information technology that collects, maintains, or disseminates information that permits identification of an individual. This includes online contact with a specific individual, if identical questions are posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the Federal Government. The PIA addresses what information is to be collected, why the information is being collected, the intended use of the information, with whom the information will be shared, what notice or opportunities for consent will be provided and how that information will be shared, secured, and whether a system of records is being created. The program or system managers are responsible for implementing the PIA in accordance with USTRANSCOM Instruction 33-11, Privacy Impact Assessment.

10. PREPARING AND PUBLISHING SYSTEM NOTICES FOR THE FEDERAL REGISTER. USTRANSCOM must publish notices in the Federal Register of new, changed, and deleted systems to inform the public of the records USTRANSCOM keeps and give them an opportunity to comment. The Privacy Act also requires submitting new or significantly changed systems to OMB and both houses of the Congress before publication in the Federal Register.

This includes starting a new system, instituting significant changes to an existing system, sending out data collection forms or instructions, and issuing a request for proposal or invitation for bid to support a new system. At least 120 days before implementing a new system of records, program or system managers must send a proposed system notice through TCJA-FO in the following format in Attachment 3. TCJA-FO will send notices to Defense Privacy and Civil Liberties Office (DPCLO) using Microsoft Word and using the Track Changes tool in Word to indicate additions/changes to existing notices. On new systems of records, system managers must include a statement that a risk assessment was accomplished and is available should OMB request it. System managers will review and validate their Privacy Act system notices annually and submit changes to TCJA-FO or processing.

11. PROTECTING AND DISPOSING OF RECORDS.

11.1. When the system becomes operational, the system manager will establish appropriate safeguards to ensure the records are secure, confidential, and protected against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The system manager will be responsible for data retained in the system of records, ensuring information maintained is current, and security procedures are complied with.

11.2. Information will be protected according to its sensitivity level. Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records is FOUO. Contact TCJ3-FP for protection methods of FOUO material. Use of AF Visual Aid 33-276 *(Air Force Privacy Label)* on file folders (affixed to the folder tab, next to the file folder label) is optional. Use computer tapes (affix to the computer tape disk reel); hard disk drive (affix to disk drive housing); and CD-ROM (affix to jewel box) to protect Privacy Act material. The AF Form 3227, *Privacy Act Cover Sheet*, or DD Form 2923, *Privacy Act Data Cover Sheet* is used for protecting Privacy Act material such as letters, file folders, listings, etc; handcarrying material to and from offices; and working with Privacy Act material at workstations.

11.3. Balance additional protection against risk and cost. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty.

11.4. A Privacy Act case file will include requests from and replies to individuals on whether a system has records about them; requests for access or amendment; approvals, denials, appeals, and final review actions; and coordination actions and related documents. Do not keep copies of disputed records in the Privacy Act case file. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document reasons for untimely responses.

11.5. Records must be transferred in a manner that prevents unauthorized disclosure of information contained in a system of records. Use sealed opaque envelopes to transfer Privacy Act material by mail. Use sealed opaque envelopes or affix a label over the string closure of

Optional Form 65-B (holey-joe) to transfer inter-base and inter-office Privacy Act material. Do not transmit a record from a system of records orally (by telephone or otherwise) to anyone unless the disclosure is authorized under the Privacy Act and until the recipient's identity and need to know are fully verified. Store paper record material or electronic media (floppy disks, CD-ROM disks, computer tapes, etc.) in a lockable container (filing cabinet, desk, etc.), or in a secured room at all times when not in use during working hours, and at all times during nonworking hours. Local Area Network (LAN) access of Privacy Act protected files will be password protected with a log-on protocol authorized by the respective system manager. Do not leave Privacy Act records unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons. Annotate each page of a document containing Privacy Act material with the statement, *"Personal Data – Privacy Act of 1974 Applies."* (This includes correspondence containing SSNs.) Mark all rosters/listings, which contain personal information (home address, home telephone number, or SSN) *"For Official Use Only (FOUO)"* and add one of the following statements:

11.5.1. Official, used for alert, recall, emergency notification, etc.: *"This (roster/listing) contains personal information and is to be used for official purposes only."*

11.5.2. Unofficial, used for social, special events planning: *"This (roster/listing) contains personal information and is to be used for social or quasi-social, special events planning purposes. Written consent has been secured from each individual listed."*

11.6. Within USTRANSCOM, destroy Privacy Act material by tearing into small pieces, shredding, or chemical decomposition to render material unrecognizable or beyond reconstruction. The destroyed material may then be placed in trash containers. USTRANSCOM *will not use recycling* as a method of destroying Privacy Act material. Clear magnetic tapes or other magnetic medium by degaussing, overwriting, or erasing. It is the system manager's responsibility to ensure this process is accomplished.

12. PRIVACY ACT EXEMPTIONS. A system manager who believes that a system of records needs an exemption from some or all of the requirements of the Privacy Act should send a request to the Defense Privacy and Civil Liberties office through the TCJA-FO. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection. Denial authorities can withhold records using these exemptions only if they were previously approved and published as an exemption for the system in the Federal Register. Exemption types include:

12.1. General exemptions free a system from most parts of the Privacy Act.

12.2. Specific exemptions free a system from only a few parts.

12.3. Approved exemptions exist under 5 United States Code 552a for:

12.3.1. Certain systems of records used by activities whose principal function is criminal law enforcement (subsection [j][2]). The following Air Force Systems of Records are exempt under 5 United States code (U.S.C.) Section 552a [j][2]:

12.3.1.1. F031 AF SP A, Correction and Rehabilitation Records (parts may be exempt).

12.3.1.2. F031 AF SP B, Security Forces Management Information System (parts may be exempt).

12.3.1.3. F051 AF JA I, Military Justice and Magistrate Court Records (parts may be exempt).

12.3.1.4. F071 AF OSI A, Counter Intelligence Operations and Collection Records (parts may be exempt).

12.3.1.5. F071 AF OSI C, Criminal Records (parts may be exempt).

12.3.1.6. F071 AF OSI D, Investigative Information Management System (parts may be exempt).

12.3.1.7. F090 AF IG B, Inspector General Records (parts may be exempt).

12.3.2. Classified information in any system of records (subsection [k][1]).

12.3.3. Law enforcement records (other than those covered by subsection [j][2]). The Air Force must allow an individual access to any record issued to deny rights, privileges or benefits to which he or she would otherwise be entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source) (subsection [k][2]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [2]:

12.3.3.1. F 031 497IG A, Sensitive Compartmental Information (SCI) Personnel Records (parts may be exempt).

12.3.3.2. F 036 AF DPG, Military Equal Opportunity and Treatment (parts may be exempt).

12.3.3.3. F 044 AF SG Q, Family Advocacy Program Records (parts may be exempt).

12.3.3.4. F051 AF JA I, Military Justice and Magistrate Court Records (parts may be exempt).

12.3.4. Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection [k][4]).

12.3.5. Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection [k][5]). The following Air Force Systems of Records are exempt under 5 U.S.C Section 552a [k] [5]:

12.3.5.1. F 031 497IG A, Sensitive Compartmental Information (SCI) Personnel Records (parts may be exempt).

12.3.5.2. F 031 497IG B, Special Security Case Files (parts may be exempt).

12.3.5.3. F 031 AF SP N, Special Security Files (parts may be exempt).

12.3.5.4. F 036 AETC I, Cadet Records (parts may be exempt).

12.3.5.5. F 044 AF SG Q, Family Advocacy Program Records (parts may be exempt).

12.3.5.6. F 071 AF OSI F, Investigative Applicant Processing Records (parts may be exempt).

12.3.6. Qualification tests for appointment or promotion in the Federal service if access to this information would compromise the objectivity of the tests (subsection [k][6]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [6]:

12.3.6.1. F 036 AFPC K, Enlisted Promotion Testing Record (parts may be exempt).

12.3.7. Information, which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection [k][7]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [7]:

12.3.7.1. F 036 AF PC A, Effectiveness/Performance Reporting Records (parts may be exempt).

12.3.7.2. F 036 AF PC O, General Officer Personnel Data System (parts may be exempt).

12.3.7.3. F 036 USAFA A, Cadet Personnel Management System (parts may be exempt).

12.3.7.4. F 036 USAFA B, Master Cadet Personnel Record (parts may be exempt).

12.3.7.5. F 036 USAFA K, Admissions Records (parts may be exempt).

13. DISCLOSING RECORDS TO THIRD PARTIES

13.1. Before releasing personal information to third parties, consider the consequences, check accuracy, and make sure that no law or directive bans disclosure. Personal information can be released to third parties when the subject agrees orally or in writing. Before including personal information such as home addresses, home phones, and similar information on social rosters or directories, ask for written consent statements. Otherwise, do not include the information.

13.2. You must get written consent before releasing a SSN, DoD Identification Number, marital status, number and sex of dependents, race, civilian educational degrees and major areas of study (unless the request for information relates to the professional qualification for federal employment), school and year of graduation, home of record, home address and phone/mobile numbers, age and date of birth, present or future assignments for overseas or for routinely

deployable or sensitive units, and office and unit address and duty phone for overseas or for routinely deployable or sensitive units. *(Note: These are not all inclusive.)*

13.3. Consent is not required to release name, rank, and grade; service specialty codes; pay (including base pay, special pay, and all allowances except Basic Allowance for Housing); gross salary for civilians; past duty assignments, unless sensitive or classified; present and future approved and announced stateside assignments; position title, office, unit address, and duty phone number; date of rank; date entered on active duty; pay date; source of commission; professional military education; promotion sequence number; military awards and decorations; duty status of active, retired, or reserve; active duty official attendance at technical, scientific, or professional meetings; biographies and photos of key personnel; and date of retirement/ separation.

13.4. Information that can be obtained by authorized individuals for official purposes on a need to know basis from existing systems of records in USTRANSCOM include:

13.4.1. Miscellaneous personnel management actions (alert or recall rosters; wartime, mobility, emergency actions or assignments; shelter duties or assignments, etc.); off-duty employment information; and *ON A VOLUNTARY PROVIDED BASIS ONLY*, an individual's involvement in off-duty activities for rendering performance/evaluation reports.

13.4.2. Dependent (spouse and children) information (name, age, sex, nationality, home address, home telephone number, etc., and special needs such as availability of special education or treatment facilities. (*NOTE: Dependent information used for unofficial or quasi-official use will be ON A VOLUNTARILY PROVIDED BASIS ONLY.)*

13.5. Information for social rosters (name, address, phone number, official title or position; invitations, acceptance, regrets, protocol) to include dependent information will be obtained *ON A VOLUNTARILY PROVIDED BASES ONLY*.

13.6. Information for special events planning (biographical data including, but not limited to: name, duty, and home address) telephone numbers; name of spouse and family; description of position in business and community affiliations with military-oriented civic organizations; and photos will be *ON A VOLUNTARILY PROVIDED BASIS ONLY*.

13.7. When disclosing other information, consider if the subject would have a reasonable expectation of privacy in the information requested, and would disclosing the information benefit the general public? USTRANSCOM considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency, or performance of its statutory duties. Balance the public interest against the individual's probable loss of privacy. Do not consider the requester's purpose, circumstances, or proposed use.

13.8. USTRANSCOM may release information without consent to:

13.8.1. Respond to FOIA requests when information is releasable.

13.8.2. Officials or employees within DOD with a need to know.

13.8.3. Agencies outside DOD for a routine use published in the Federal Register. The purpose of the disclosure must be compatible with the purpose in the routine use. When initially collecting the information from the subject, the "Routine Uses" block in the Privacy Act Statement must name the agencies and reason.

13.8.4. The Bureau of the Census to plan or carry out a census or survey under Title 13, United States Code, Section 8.

13.8.5. A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. (*NOTE: No one may use any part of the record to decide an individual's rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.)*

13.8.6. The Archivist of the United States and the National Archives and Records Administration to evaluate records for permanent retention.

13.8.7. A federal, state, or local agency (other than DOD) for civil or criminal law enforcement. TCJA or TCJA-D must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a routine use for all DOD systems of records and is published in the Federal Register.

13.8.8. An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

13.8.9. Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

13.8.10. A congressional office acting for the record subject. A published, blanket routine use permits this disclosure. If the material for release is sensitive, obtain a release statement first.

13.8.11. The Comptroller General or an authorized representative of the General Accounting Office on business.

13.8.12. A court order of a court of competent jurisdiction, signed by a judge.

13.8.13. A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a routine use.

13.9. Service personnel may disclose the medical records of minors to their parents or legal guardians. The laws of each state define the age of majority. Services must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's

medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

13.10. Systems managers must keep an accurate record of all disclosures made from any system of records except disclosures to DOD personnel for official use or disclosures under the FOIA. Use Air Force Form 771, *Accounting of Disclosures,* for record disclosure tracking. *(NOTE: Disclosure of personal records to a contractor for use in the performance of a USTRANSCOM contract is considered a disclosure within the agency.)*

14. COMPUTER MATCHING PROGRAMS. Computer matching programs electronically compare records from two or more automated systems that may include DOD, another Federal agency, or a state or other local government. Proposed matches that could result in an adverse action against a Federal employee must meet the following requirements: a written agreement between participants, approval of the Defense Data Integrity Board, matching notice published in Federal Register before matching begins; full investigation and due process enforced, and act on the information, as necessary. The Privacy Act applies to matching programs that use records from Federal personnel or payroll systems and Federal benefit programs where matching determines Federal benefit eligibility, checks on compliance with benefit program requirements, recovers improper payments or delinquent debts from current or former beneficiaries. Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that will not cause any adverse action are exempt from the Privacy Act matching requirements. Contact TCJ6-DI before participating in a matching program. *(NOTE: Allow 180 days for processing requests for a new matching program.)*

15. PRIVACY AND THE WEB. *Do not* post personal information on publicly accessible DOD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, *do not* post personal information on non-publicly accessible web sites unless it is mission essential and appropriate safeguards have been established. Public web sites will comply with privacy policies regarding restrictions on persistent and third party cookies, and appropriate privacy and security notices at major web site entry points will be added as well as Privacy Act statements or Privacy Advisories when collecting personal information. A Privacy Act Statement will be included on the web page that collects information directly from an individual, and that information is maintained and retrieved by an individual's personal identifier (i.e., SSN). Personal information will be maintained only in approved Privacy Act systems of records that are published in the Federal Register. Anytime a web site solicits personally-identifying information, even when not maintained in a Privacy Act system of records, it requires a Privacy Advisory, which informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the web page where the information is being solicited or through a well-marked hyperlink *"Privacy Advisory – Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used."*

16. TRAINING. The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel

specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. The aforementioned personnel are required to have annual Privacy Act (Identifying & Safeguarding Personally Identifiable Information) training.

17. INFORMATION COLLECTIONS, RECORDS, AND FORMS OR INFORMATION MANAGEMENT TOOLS.

17.1. No information collections are required by this publication.

17.2. Retain and dispose of Privacy Act records according to CJCSM 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures, and Volume II, Disposition Schedule.

MICHAEL J. BENJAMIN
Colonel, U.S. Army
Staff Judge Advocate

Attachments
1. Glossary of References, Abbreviations, Acronyms, and Terms
2. Sample Privacy Act Statement (PAS)
3. Template for Preparing a Privacy Act System Notice

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A – References

Executive Order 9397, 22 November 1943, Numbering System for Federal Accounts Relating to Individual Persons
32 Code of Federal Regulations 806b-1354, Air Force Privacy Act Program
Title 5, United States Code, Section 552, The Freedom of Information Act
Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974
Title 10 United States Code, Section 164, Armed Forces, Organization and General Military Powers, Combatant Commands
Title 10 United States Code, Section 3013, Armed Forces Organization, Department of the Army
Title 10 United States Code, Section 5013, Armed Forces Organization, Department of the Navy
Title 10 United States Code, Section 8013, Armed Forces Organization, Department of the Air Force
Title 13 United States Code, Section 8, Census, Administration, General Provisions
Public Law 100-235, The Computer Security Act of 1987
Public Law 100-503, The Computer Matching and Privacy Act of 1988
Public Law 104-13, Paperwork Reduction Act of 1995
Public Law 107-347, Section 208, Electronic Government Act of 2002
Chairman Joint Chiefs of Staff Manual 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule
Department of Defense 6025.18-R, DOD Health Information Policy Regulation
Department of Defense Directive 5400.11, Department of Defense Privacy Program
Department of Defense 5400.11-R, Department of Defense Privacy Program
Department of Defense Instruction 1000.30, Reduction of SSN use Within DoD
Air Force Instruction 33-332, Air Force Privacy Act Program
USTRANSCOM Instruction 33-11, Privacy Impact Assessment
USTRANSCOM Instruction 33-26, USTRANSCOM Freedom of Information Act Program

Section B - Abbreviations and Acronyms

AF	Air Force
AF-CIO-P	Air Force Chief Information Officer - Privacy
DOD	Department of Defense
CIO	Chief Information Officer
CJCSM	Chairman Joint Chiefs of Staff Manual
CPF	Civilian Personnel Flight
E-Government	Electronic Government
E-Mail	Electronic Mail
FOIA	Freedom of Information Act
FOUO	For Official Use Only
OMB	Office of Management and Budget
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
SSN	Social Security Number

TCJ3-FP	USTRANSCOM Force Protection
TCJA	USTRANSCOM Staff Judge Advocate
TCJA-D	USTRANSCOM Deputy Staff Judge Advocate
TCJA-FO	USTRANSCOM Privacy Act Officer
TCJ6	USTRANSCOM Command, Control, Communications and Computer Systems Directorate
USTRANSCOM	United States Transportation Command

Section C - Terms

Access. Allowing individuals to review or receive copies of their records.

Agency. For the purposes of disclosing records subject to the Privacy Act among Department of Defense (DOD) Components, the DOD is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and recordkeeping as regards release to non-DOD agencies; each DOD Component is considered an agency within the meaning of the Privacy Act.

Amendment. The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer Matching. A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity will not be disclosed or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

Confidentiality. An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identify of confidential sources.

Denial Authority. The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead

person under this instruction and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

Individual Access. To make available information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Maintain. Includes collecting, safeguarding, using, accessing, amending, and disseminating personal information.

Matching Agency. The agency that performs a computer match.

Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor. Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Official Use. Within the context of this instruction, this term is used when employees of a DOD component have a demonstrated need for the use of any records or the information contained therein in the performance of their authorized duties.

Personal Identifier. A name, number, or symbol which is unique to an individual, usually the person's name or Social Security Number (SSN).

Personal Information. Knowledge about an individual that is intimate or private to the individual, as distinguished from that related solely to the individual's official functions or public life.

Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Privacy Act Statement (PAS). A statement furnished to an individual when the individual is requested to provide personal information, regardless of the medium used to collect the information, to go into a system of records. A PAS is also furnished to an individual when asking them for their SSN.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new system of records is being created under the Privacy Act.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions,

medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use. The disclosure of a record outside the DOD for a use that is compatible with the purpose for which the information was collected and maintained by the DOD. The routine use must be included in the published system notice for the system of records involved. For example: "To the Veterans Administration to verify the physical disability of applicants for the purpose of authorizing monthly retirement disability payments."

Source Agency. A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager. The individual who initiates a system of records, operates such system, or is responsible for a segment of a decentralized part of that system and issues policies and procedures for operating and safeguarding of information in the system.

System Notice. The official public notice published in the Federal Register of the existence and content of the system of records.

System of Records. A group of records under the control of a DOD component from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual and published in the Federal Register.

Attachment 2

SAMPLE PRIVACY ACT STATEMENT

JOINT PERSONNEL SYSTEM

AUTHORITY: Title 5 United States Code, Section 301; Title 10 United States Code, Sections 164, 3013, 5013, and 8013; Executive Order 9397.

PURPOSES: To provide USTRANSCOM Commander, Deputy Commander, Chief of Staff, element commanders, directors, chiefs of direct reporting elements, functional managers, and supervisors: (1) A ready source of information for day-to-day operations and administrative determinations pertaining to assigned personnel, (2) A protocol listing to include spouses' names for social/special events planning. Use of the SSN is necessary for establishing a record and identification control in the automated system.

ROUTINE USES: Information will not be released outside of the Department of Defense.

DISCLOSURE: Voluntary: (1) The furnishing of civilian/military member information is voluntary; but failure to provide it may result in your not receiving/could hamper/could delay personnel support. (2) The furnishing of dependent information is voluntary.

Attachment 3

SAMPLE
(Reference DOD 5400.11-R, Chapter 6)

NEW SYSTEMS OF RECORDS NOTICE (SORN)

New Systems of Records Notice

System Location:
Defense Enterprise Computing Center, 5450 Carlisle Pike, Mechanicsburg PA 17055
Backup Location: Defense Enterprise Computing Center, 7879 Wardleigh Road, Building 891, Hill AFB UT 84056.

Categories of individuals covered by the system:
Individuals traveling in the Defense Transportation System (Air, Land, or Sea). Passengers include military personnel, dependents, medical patients/evacuees, and DOD civilians.

Authority for maintenance of the system:
Executive Order 9397 as implemented by Department of Defense Directive 5400.11, DOD Privacy Program, and Department of Defense Regulation 5400.11, DOD Privacy Program, and Department of Defense Regulation 4500.9, Defense Transportation Regulation, and E.O. 9397 (SSN).

Purposes:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To provide United States Transportation Command (USTRANSCOM) visibility of cargo and personnel movement within the Defense Transportation System.

Routine Uses of records maintained in the system, including categories of users and the purposes of such uses:

To disclose information to a Federal agency in order to manage and optimize military transportation resources.

To disclose information to a Federal agency to track and locate individuals moving within the Defense Transportation System.
To disclose information to a Federal agency for accumulating reporting data and monitoring of the system.

The DOD "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Records are maintained on electronic storage media.

Retrievability:

Query by passenger name, SSN, reservation number, or location. Query results: Name, SSN, Rank.

Query by mission number. Query results: Number of passengers on mission.

Query on passenger number. Query results: Name, Rank, Gender, SSN, Blood Type, Unit Identification Code (IUC) and Unit Line Number (ULN).

Query by IUC or ULN. Query results: Name, SSN, Service, Gender.

Safeguards:
Access to computerized data is restricted by passwords which are changed periodically.

Retention and disposal:
Retention will be in accordance with Chairman Joint Chiefs of Staff Manual (CJCSM) 5760.01 Volume II, Joint Staff and Combatant Command Records Management Manual – Disposition Schedule. *Erase* individual records when superseded or obsolete. Authority: N1-218-89-2 item 9 (temporary transaction).

System Manager and address:
Defense Logistics Agency (Integrated Data Environment/Global Transportation Network Convergence (IGC) Program Manager, J-626, 8725 John J. Kingman Road, Fort Belvoir VA 22060

Notification procedure:
Individuals seeking to determine whether information about them is contained in this system should address written inquiries to Defense Logistics Agency, J-626, IGC Program Manager, 8725 John J. Kingman Road, Fort Belvoir VA 22060
Request should contain full name and social security number (SSN).

Contesting record procedures:
The OSD's rules for assessing records, for contesting contents an appealing initial agency determinations are published in OSD Administrative Instruction No. 81; 32 CFR part 311; or may be obtained from the system manager.

SAMPLE
(Reference DOD 5400.11-R, Chapter 6)

DEPARTMENT OF DEFENSE
Office of the Secretary
Narrative Statement on a [New/Altered] System of Records
Under the Privacy Act of 1974

1. System identifier and name: DITPR ID 8867 and CPA 490, entitled "Integrated Data Environment/Global Transportation Network Convergence (IGC)" [replacement for the Global Transportation Network (GTN) IT System].

2. Responsible official: Lieutenant Colonel Ronald Emerson, U.S. Army, United States Transportation Command, Directorate of Command, Control, Communications & Computer Systems (USTRANSCOM/TCJ6), 508 Scott Drive, Scott Air Force Base IL 62225-5357

3. Purpose of establishing the system: Tracking of cargo and personnel moving within the Department of Defense (DOD) Defense Transportation System (DTR).

4. Authority for the maintenance of the system: DOD Regulation 4500.9, Defense Transportation System, and E.O. 9397 (SSN).

5. Probable or potential effects on the privacy of individuals: None.

6. Is the system, in whole or in part, being maintained by a contractor: Yes (In part).

7. Steps taken to minimize risk of unauthorized access: Access is restricted by password. Data located in restricted access-controlled facilities. Common Access Card (CAC) log-on/authentication will be implemented into IGC from the program standup. Log-in accounts will be validated on a regular basis to insure minimal risk of compromised accounts.

8. Routine use compatibility: Any release of information contained in this system of records outside of the DOD will be compatible with purposes for which the information is collected and maintained. The DOD "Blanket Routine Uses" apply to this system of records.

9. OMB information collection requirements: None

10. Supporting documentation: None.

SAMPLE
(Reference DOD 5400.11-R, Chapter 6)

Altered System of Records Notice (SORN)

* * * * *
System identifier:
Replace "S253.10 DLA-G" with "S100.70."

* * * * *

Categories of individuals covered by the system:
Delete "to the DLA General Counsel" at the end of the sentence and replace with "to DLA."
* * * * *

Categories of records in the system:
Delete entry and replace with Inventor's name, Social Security Number, address and telephone number(s); descriptions of inventions; designs or drawings, as appropriate; evaluations of patentability; recommendations for employee awards; licensing documents; and similar records. Where patent protection is pursued by DLA, the file may also contain copies of applications, Letters Patent, and related materials.

* * * * *

Authority for maintenance of the system:
Delete entry and replace with 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 4502, General provisions; 10 U.S.C. 2320, Rights in technical data; 15 U.S.C. 3710b, Rewards for scientific, engineering, and technical personnel of federal agencies; 15 U.S.C. 3711d, Employee activities; 35 U.S.C. 181-185, Secrecy of Certain Inventions and Filing Applications in Foreign Countries; E.O. 9397 (SSN); and E.O. 10096 (Inventions made by Government Employees) a amended by E.O. 10930.

* * * * *

Purpose(s):
Delete entry and replace with "Data is maintained for making determinations regarding and recording DLA interest in the acquisition of patents; for documenting the patent process; and for documenting any rights of the inventor. The records may also be used in conjunction with the employee award program, where appropriate."

* * * * *

Routine uses of records maintained in the system, including categories of users and the purpose of such uses:

Add two new paragraphs "To the U.S. Patent and Trademark Office for use in processing applications and performing related functions and responsibilities under title 35 of the U.S. Code.

To foreign government patent offices for the purpose of securing foreign patent rights."

* * * * *

Safeguards:
Delete entry and replace with "Access is limited to those individuals who require the records for the performance of their official duties. Paper records are maintained in buildings with controlled or monitored access. During non-duty hours, records are secured in locked or guarded buildings, locked offices, or guarded cabinets. The electronic records systems employ user identification and password or smart card technology protocols."

* * * * *

Retention and disposal:
Delete entry and replace with "Records maintained by Headquarters and field offices are destroyed 26 years after file is closed."

* * * * *

Records source categories:
Delete entry and replace with "Inventors, reviewers, evaluators, officials of U.S. and foreign patent offices, and other persons having a direct interest in the file."

* * * * *

S100.70

System name:

System location:

Categories of individuals covered by the system:

Categories of records in the system:

Authority for maintenance of the system:

Purpose(s):

The DOD "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:
Records are maintained in paper and computerized form.

Retrievability:
Files by name and SSN

Safeguards:
Access is limited to those individuals who require the records for the performance of their official duties. Paper records are maintained in buildings with controlled or monitored access. During non-duty hours, records are secured in locked or guarded buildings, locked offices, or guarded cabinets. The electronic records systems employ user identification and password or smart card technology protocols.

Retention and disposal:

System manager(s) and address:
United States Transportation Command (USTRANSCOM)
Directorate of Command, Control, Communications & Computer Systems (TCJ6)
Attn: TCJ6-T
508 Scott Drive
Scott AFB IL 62225-5257

Notification procedures:
Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to command Privacy Act Officer (USTRANSCOM/TCCS-DI), 508 Scott Drive, Scott AFB IL 62225-5257.

Individuals should provide information that contains full name, current address and telephone number(s) of requester.

For personal visits, each individual shall provide acceptable identification, e.g., driver's license or identification card.

Contesting record procedures:
Air Force CIO (SAF/XCPPA), 1000 AF Pentagon, Washington, DC 20330-1000

Record source categories:
Inventors, reviewers, DOD representatives, and other persons having a direct interest in the file.

Exemptions claimed for the system:
None.