



PRIVACY ACT AND CIVIL LIBERTIES 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 Eric J. Werner, USAF)

Supersedes: USTRANSCOMI 33-35, 18 November 2014

Pages: 35

Distribution: e-Publishing

This instruction establishes policies, procedures, and responsibilities for implementing the United States Transportation Command (USTRANSCOM) Privacy Act and Civil Liberties Program. The Privacy Act Program safeguards personally identifiable information (PII) protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013, and collected and maintained in USTRANSCOM systems of records. All Information Technology (IT) systems that collect, maintain, or disseminate PII are covered by the Privacy Act System of Records Notice (SORN), FTRANSCOM 01 DoD. This SORN is available at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/COCOM-Article-List/>

This instruction is applicable to all personnel assigned to USTRANSCOM. Failure to obey a regulation is a violation of the Uniform Code of Military Justice (UCMJ) for military personnel. Civilian employees may receive an administrative disciplinary action applicable to criminal or civil sanctions under related laws. 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 and Civil Liberties Program.

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. 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 (SOR) that doesn't meet the public notice requirements; disclosing information from a SOR 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, *Records Management*.

SUMMARY OF REVISIONS

This instruction was revised to include USTRANSCOM civil liberties program.

TABLE OF CONTENTS

Chapter 1 - REFERENCES AND SUPPORTING INFORMATION	3
Chapter 2 - PURPOSE OF PRIVACY ACT PROGRAM	3
Chapter 3 - APPLICABILITY	3
Chapter 4 - DEFINITION	3
Chapter 5 - POLICY	3
Chapter 6 - RESPONSIBILITIES	3
6.1. LIMIT THE COLLECT OF PERSONAL INFORMATION.....	4
6.1.1. USTRANSCOM System of Records.....	4
6.1.2. System of Records Operated By a Contractor.....	4
6.1.3. Other Agencies' SORN.....	4
6.1.4. Reduction of SSN Use Within DoD.....	4
6.1.5. Exercise of First Amendment rights.....	5
6.1.6. Personal Notes.....	5
6.1.7. Medical Information.....	5
6.1.8. Unit Personnel Rosters.....	5
6.1.9. Collecting PII from Third Parties.....	5
6.1.10. Safeguarding Collected PII.....	6
6.2. INFORM INDIVIDUALS OF THE PURPOSE AND USE OF INFORMATION	8
6.2.1. Privacy Act Statement.....	8
6.2.2. Privacy Impact Assessment.....	9
6.2.3. PII Breach.....	9
6.2.4. Privacy Act Requests.....	10
6.2.5. Computer Matching.....	12
6.3. PUBLISH A SYSTEMS OF RECORDS NOTICE	13
6.3.1. The Process of Publishing a SORN.....	13
6.4. PRIVACY ACT COMPLAINTS AND VIOLATIONS	14
Chapter 7 – ROLES	14
7.1. USTRANSCOM PRIVACY ACT PROGRAM MANAGER	14
7.2. SENIOR COMPONENT OFFICIAL FOR PRIVACY	16
7.3. SYSTEM MANAGERS	16
Chapter 8 - PURPOSE OF CIVIL LIBERTIES PROGRAM	18
Chapter 9 - APPLICABILITY	18
Chapter 10 - DEFINITION	18
Chapter 11 - POLICY	18
Chapter 12 - RESPONSIBILITIES	18
Chapter 13 - RELEASABILITY	20
Attachment 1.....	21
Attachment 2.....	25
Attachment 3.....	26
Attachment 4.....	27

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

2. PURPOSE OF PRIVACY ACT PROGRAM. This instruction, in accordance with DoD Directive 5400.11, establishes policy and procedures for the implementation of United States Transportation Command's (USTRANSCOM) Privacy Act Program.

3. APPLICABILITY. This instruction applies to all USTRANSCOM directorates/staff offices, joint task force headquarters, and other assigned activities and associated units under the support or control of USTRANSCOM.

4. DEFINITION. Privacy. The right to be free from unwanted or undue intrusion or disturbance from secret surveillance or unauthorized disclosure of one's personal data or information recognized under the Privacy Act of 1974 as amended.

5. POLICY. It is USTRANSCOM policy to protect and safeguard an individual's fundamental legal right to privacy.

5.1. USTRANSCOM must collect, maintain, and use PII in order to carry out its essential mission or functions. When collecting PII all individuals will be informed why the information is needed. The collected PII will be maintained in a system of records (SOR). A SOR is a grouping of records under the control of a Federal government agency that can retrieve PII by an individual's name, Social Security number (SSN), or other personal identifiers.

5.2. Under the Privacy Act of 1974, USTRANSCOM must provide certain safeguards for their SOR in order to protect individuals against an invasion of personal privacy. PII collected and maintained in a SOR will be protected by using appropriate administrative, technical, and physical safeguards. In addition, the public will be made aware of any SOR by notice in the Federal Register.

5.3. Disclosure of individual's records in a SOR must first have written consent or as otherwise authorized by Title 5, United States Code, section 552a, *as amended, The Privacy Act of 1974*, Records maintained on individuals.

5.4. Only records that are relevant and necessary to accomplish USTRANSCOM's missions or functions will be maintained in a SOR. Records that are no longer relevant or necessary must be deleted and/or destroyed. For disposition instructions reference USTRANSCOM Instruction 33-32, Records Management.

5.5. This instruction applies to information contained in USTRANSCOM's SOR.

6. RESPONSIBILITIES. The Privacy Act of 1974 requires USTRANSCOM to: limit the collection of personal information, inform individuals of the purpose and use of information, and publish a Systems of Records Notice. If the Privacy Act of 1974 provisions are violated, an individual may seek relief through appropriate channels or in court.

6.1. LIMIT THE COLLECT OF PERSONAL INFORMATION. The collection and use of personal information must continually be justified and reexamined in order to safeguard PII, and to maintain accurate, relevant, timely, and complete information.

6.1.1. USTRANSCOM System of Records (SOR). USTRANSCOM SOR can only collect and maintain records as described in the Privacy Act SORN, FTRANSCOM 01 DoD. Personal information that has been approved under this notice are individual's name, rank, unit, identification code, Service affiliation, personal identifiers (such as SSN, DoD Identification Number, Employee Identification Number, military identification, passport number, blood type, driver's license number, address, telephone number, electronic mail (e-mail) address, emergency contact information) and other information relating to movement of individuals and personal property in the Defense Travel System (DTS). PII should only be collected 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.

6.1.1.1. Maintaining a SOR on individuals without their knowledge and/or without a SORN published to the Federal Register is known as maintaining a "Secret File," which is a violation of the Privacy Act. Personnel who fail to adhere to this paragraph may be punished under the Uniform Code of Military Justice, Article 92, or civil equivalent.

6.1.2. SOR Operated By a Contractor. Contractors who are required to operate or maintain a Privacy Act SOR 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.

6.1.3. Other Agencies' SORN. USTRANSCOM personnel must comply with all SORNs. SORNs are published in the Federal Register at <https://www.federalregister.gov>.

6.1.4. Reduction of SSN Use Within DoD. USTRANSCOM is required to reduce or eliminate SSNs by continuous justifying and reexamining the acceptable uses outlined in Department of Defense Instruction (DoDI) 1000.30, *Reduction of SSN Use Within DoD*, Enclosure 2, paragraph 2.

6.1.4.1. DoD SSN Justification Memorandum and Form. Continual justification of SSNs is conducted bi-annually by submitting a SSN Justification Memorandum to the Defense Privacy and Civil Liberties Office. The memorandum must name the IT systems or forms that are the subject of the justification and reference the SORN, Privacy Impact Assessment (PIA), or any documentation to indicate what actions are being taken to reduce the vulnerability of SSNs. If a new form is needed to collect PII, use DD Form 67. The DoD SSN Justification Memorandum template and instructions can be found under DoDI 1000.30, Enclosure 4, Figure 1., Sample SSN Justification Memorandum.

6.1.4.2. Plan to Eliminate Use of the SSN. USTRANSCOM personnel shall make a continual effort to reduce or eliminate the use of SSNs wherever possible. This includes truncated (last four), masked, partially masked, encrypted, or disguised SSNs.

6.1.4.2.1. If the justification of using SSNs is not approved by DoD then it must be eliminated. A plan to eliminate the use of the SSN will include; a reasonable timeframe in order to reduce the impact on operations and decrease overall cost; the alternative identification number to replace the SSNs being used; a list of the forms and systems being affected by the elimination; and the mitigation strategy detailing efforts made by owners of the systems and/or forms being affected. Refer to DoDI 1000.30, Enclosure 4, Figure 2, for the sample SSN Elimination Plan.

6.1.5. Exercise of First Amendment rights. A record of anyone exercising their First Amendment rights will not be maintained by USTRANSCOM unless expressly authorized by Federal statute, the individual, or within the scope of an authorized law enforcement activity.

6.1.5.1. USTRANSCOM will not penalize or harass an individual for exercising rights guaranteed under the Privacy Act and will give reasonable aid to individuals exercising their rights.

6.1.6. 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.

6.1.7. Medical Information. Service element commanders, directors, Command Support Group (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.

6.1.7.1. Service personnel may disclose 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.

6.1.8. Unit Personnel Rosters. Before including personal information for the following; alert, recall rosters, wartime, mobility, emergency actions, assignments, shelter duties, social rosters, special events planning , etc., such as home addresses, home phones, dependent's information and similar information; ask for written consent statements telling the individual that disclosing this information is voluntary.

6.1.9. Collecting PII from Third Parties. Collection of PII from third parties sources is practicable when:

6.1.9.1. Security or employment suitability determinations.

6.1.9.2. Supervisor's comments on job knowledge, duty performance, or other opinion-type evaluations.

6.1.9.3. Investigative inquiry into the actions of the individual.

6.1.9.4. Permission from the individual to furnish exact periods of employment, termination dates, copies of records, or similar information.

6.1.10. Safeguarding Collected PII. All USTRANSCOM personnel and authorized personnel; Service Element Commanders, Directors, CSG Chiefs, Functional Managers, and Supervisors, who obtain PII for official purposes on a need to know basis, are responsible for ensuring Privacy Act data, under their control, is safeguarded and must comply with the following:

6.1.10.1. Labeling PII. Labeling PII with a Privacy Act label is mandatory to assist in identifying Privacy Act information in order to ensure its protection.

6.1.10.1.1. The AF Visual Aid 33-276 (Air Force Privacy Act Label) will be used on: file folders (affixed to the folder tab, next to the file folder label); 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.

6.1.10.1.2. 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; hand-carrying material to and from offices; and working with Privacy Act material at workstations.

6.1.10.2. Marking PII. Mark Privacy Act documents by annotating on the top and bottom of each page with the statement, "For Official Use Only-Privacy Act of 1974."

6.1.10.2.1. Mark all rosters including recall, alert, emergency notification, social, and special events planning, etc., with, "For Official Use Only-Privacy Act of 1974." Written consent must be secured from each individual before listed on any roster.

6.1.10.3. Transporting Privacy Data. The following are ways to safeguard PII against lost, theft, and/or compromise.

6.1.10.3.1. Via Telephone. Do not transmit a record from a SOR 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.

6.1.10.3.2. Via Ground Mail. Use sealed opaque envelopes to transfer Privacy Act material by mail. Place an Air Force Privacy Act Label in the inner envelope to protect the data within. Never indicate on the outer envelope that the letter contains Privacy Act data.

6.1.10.3.3. Via E-mail. Exercise caution before transmitting PII over 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.

6.1.10.3.3.1. When sending PII 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.

6.1.10.3.3.2. 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.”

6.1.10.3.3.2.1. Ensure records promised confidentiality in an e-mail are exempt from disclosure under Title 5, United States Code, section 552a, Subsection (k)(2), (k)(5), or (k)(7) of the Privacy Act. Never e-mail PII to a personal e-mail account/address.

6.1.10.3.4. Via the Internet. Do not post personal information on publicly accessible DoD websites unless clearly authorized by law and implementing regulation and policy. Do not post or collect PII without the user’s explicit consent on social media. Additionally, do not post personal information on non-publicly accessible websites unless it is mission essential and appropriate safeguards have been established.

6.1.10.3.4.1. Public websites will comply with privacy policies regarding restrictions on persistent and third party cookies, and appropriate privacy and security notices at major website entry points will be added, as well as, Privacy Act Statements when collecting personal information.

6.1.10.3.4.1.1. A Privacy Act Statement will be included on the webpage 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 an approved Privacy Act SOR that are published in the Federal Register. Anytime a website solicits PII, even when not maintained in a Privacy Act SOR, it requires a Privacy Act Statement, which informs the individual why the information is solicited and how it will be used. Post the Privacy Act Statement to the webpage where the information is being solicited. Please refer to section 6.2.1., “Privacy Act Statement,” which will describe why this information is collected and how it will be used.”

6.1.10.4. Securing PII. 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 non-working hours. Do not leave Privacy Act records unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons.

6.1.10.4.1. Shared drives and SharePoint. PII stored on shared drives and/or SharePoint must only be visible and accessible to authorized individuals who have an official need-to-know to support the mission. Official records with PII should never be stored on shared drives or SharePoint, only in authorized SOR.

6.1.10.5. Disposing of Privacy Act Data. Retain and dispose of Privacy Act records according to CJCSM 5760.01A. It is the system manager’s responsibility to ensure this process is accomplished. See roles for more information on system manager’s roles.

6.1.10.5.1. If it is determined the Privacy Act records can be disposed of: destroy the 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 approved shred bins. USTRANSCOM will not use recycling as a method of destroying Privacy Act material. Clear magnetic tapes or other magnetic medium may be cleared by degaussing, overwriting, or erasing.

6.1.10.6. Disclosing Records to Third Parties. The Privacy Act only compels disclosure of records from a SOR to the individual to which the records pertain to.

6.2. INFORM INDIVIDUALS OF THE PURPOSE AND USE OF INFORMATION.

USTRANSCOM must inform individuals the purpose and use of PII by providing a Privacy Act Statement (PAS), regardless of medium being used, and conducting a PIA to ensure the collected PII is stored according to the applicable laws regarding privacy. If PII is lost, stolen, or compromised the command shall promptly notify the individual of the PII breach. In addition, at any time an individual may correct or request their collected personal information.

6.2.1. Privacy Act Statement. Give a PAS orally or in writing to anyone from whom personal information is collected for a SOR, and whenever an individual's SSN is requested. A PAS includes the following five items: authority, purpose, routine use(s), disclosure, and sometimes applicable SORN (See Attachment 2 for sample PAS). A Privacy Advisory is given when soliciting an individual's SSN for authentication purpose only and will not be maintained in a SOR. The Privacy Advisory will use the same format as a PAS.

6.2.1.1. Authority. The legal authority, Federal statute or executive order, allowing the solicitation of the personal information being collected.

6.2.1.2. Purpose. The principal purpose(s) will inform the individual of how the information is being used.

6.2.1.3. Routine Use(s). Routine Use(s) will list who outside of DoD USTRANSCOM will routinely share personal information. DoD has established blanket routine uses that can be used. However, "DoD Blanket Routine Uses" must be cited. A list of DoD Blanket Routine Uses are located at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>.

6.2.1.4. Disclosure. Disclosure of personal information should be voluntary unless required by law. If mandatory disclosure is required, USTRANSCOM's legal office will need to review the mandatory disclosure requirements before use on any PAS.

6.2.1.4.1. Do not disclose an individual's SSN without an official need to know, this includes disclosing to personnel in USTRANSCOM and DoD-wide. Outside DoD, SSNs are not releasable without consent pursuant to the Privacy Act of 1974, "No Disclosure Without Consent" Rule, unless authorized by the 12 exceptions. The 12 exceptions are available at: http://dpcl.d.defense.gov/Portals/49/Documents/Privacy/2011%20DPCLO_Intro_Privacy_Act.pdf.

6.2.1.5. Applicable SORN. For USTRANSCOM: FTRANSCOM 01 DoD. This SORN is available at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/COCOM-Article-List/>.

6.2.1.5.1. If USTRANSCOM is collecting information and it is not covered under this applicable SORN, then a new SORN must be conducted. See section 6.3 for details on the process.

6.2.1.5.2. If the information is not maintained by USTRANSCOM's SOR go to, <https://www.federalregister.gov/>, to find the applicable SORN.

6.2.2. Privacy Impact Assessment. PIA is an analysis of how PII is used in an IT system. The Electronic Government (E-Government) Act of 2002 and DoDI 5400.16 requires PIAs to be conducted before developing an IT system and electronic compilations that collects, uses, protects, shares, manages, maintains, or disseminates PII or when an IT system change exposes a new privacy risk.

6.2.2.1. PIAs are recorded on DD Form 2930 and addresses the following: what information is to be collected and why; the intended use of the information; with whom the information will be shared; the privacy risks involved; the safeguards in place to protect PII; what notice or opportunities for consent will be provided and how that information will be shared, secured, and whether a SOR is being created.

6.2.2.2. Safeguarding personal information is the primary goal of the PIAs. PIAs shall establish appropriate administrative, technical, and physical safeguards to protect PII from unauthorized access, alteration, or disclosure and against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

6.2.2.3. PIAs are reviewed initially and every three years to ensure collection, maintenance, use, or dissemination of PII conforms to the applicable law. PIAs must be reviewed and signed by the system's program manager, information system security manager, privacy representative, Staff Judge Advocate designee, senior information security officer, and Chief Information Officer (CIO). The CIO will serve as the final review and approval official.

6.2.2.4. After PIAs are approved, sections 1 and 2 (pages 1-6) of DD Form 2930 are published to USTRANSCOM FOIA public website at <http://www.ustranscom.mil/foia/pia.cfm>. Sections 3 and 4 of DD Form 2930 are non-releasable since they contain PII. If sections 1 and 2 contain information that would raise security concerns or reveal classified or sensitive information, then USTRANSCOM can restrict the publication of the assessment. Such information is protected under FOIA.

6.2.3. PII Breach. A breach is a loss of control, compromise, or any situation where persons other than authorized users have potential access to PII whether physical or electronic. Once a PII breach has been confirmed, notify USTRANSCOM's Privacy Act Program Manager as soon as possible.

6.2.3.1. The Privacy Act Program Manager is responsible for preparing all reports and notifying individuals of the PII breach. See roles for more information on the Privacy Act Program Manager.

6.2.4. Privacy Act Requests. Privacy Act requests are made from individuals seeking notification as to the existence of, access to, or amendment of records, pertaining to that individual.

6.2.4.1. Privacy Act request must be made in writing and describe the specific record requested. Privacy Act requests must also include a notarized statement with signature and two forms of identification in order to confirm the requester's identity. USTRANSCOM's Privacy Act Request Form is at attachment 3.

6.2.4.1.1. Verification of identity is essential in order to avoid unauthorized disclosures. If a designated representative is making a request on behalf of the individual to whom the records pertain to, a power of attorney must be submitted.

6.2.4.1.2. Using government resources, such as equipment, supplies, stationery, postage, telephones, or official mail channels, to make a Privacy Act request or amendment is not authorized.

6.2.4.1.3. In addition, the amendment process is not intended to permit the alteration of records presented in the course of judicial or quasi-judicial proceedings

6.2.4.2. Privacy Act Request Process. Privacy Act requests have to be acknowledged within 10 workdays and completed within 20 workdays. All Privacy Act requests will be considered under both FOIA and Privacy Act regardless of the Act cited. There is no requirement to cite either Act and the Privacy Act requests must be processed under whichever Act gives the most information.

6.2.4.2.1. USTRANSCOM can only process Privacy Act requests for records maintained as described in the SORN, FTRANSCOM 01 DoD. Privacy Act requests on records not being maintained in USTRANSCOM's SOR will be referred to the appropriate agency. For guidance on finding the appropriate agency, go to the Federal Register's website at <https://www.federalregister.gov/> where all Privacy Act SORNs are published.

6.2.4.2.2. Denial Authorities. USTRANSCOM Staff Judge Advocate (SJA) or Deputy SJA (in absence of SJA) are the Initial Denial Authority (IDA). Only the IDA can deny an individual access to a record or amendment.

6.2.4.2.2.1. The reason for denial must cite one of the following; was compiled in reasonable anticipation of a civil action or proceeding, contains classified information, denied by another Federal Statute, addressed in DoD 5400.11-R, *DoD Privacy Act Program*, and/or the SOR is exempted. Please note: Currently, USTRANSCOM's SOR has no exemptions claimed. However, if the SORN is updated to reflect an exemption: the Privacy Act requester will still be provided any parts that are releasable under FOIA.

6.2.4.2.2.1.1. Privacy Act Exemptions. A system manager who believes that a SOR 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 Division 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. Types of Exemptions are referenced under DoD 5400.11-R, chapter 5 at <http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf>.

6.2.4.2.3. 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.

6.2.4.2.4. 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.

6.2.4.2.5. Releasing Privacy Act Records. Privacy Act requesters will receive a release letter notifying them if their request was completed in full, partially denied, and/or denied in full. If a partial or full denial of request, the release letter must cite appeal rights and the following; date of the denial, specific reason for denial (cite appropriate exemptions from the Privacy Act), and the denial authority.

6.2.4.2.6. Amending Privacy Act Records. Privacy Act requesters will receive an amendment letter notifying them of a correction or refusal. Amendments that have been approved in full will be corrected by the systems manager. USTRANSCOM will not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. If the amendment is refused, in whole or in part, the letter must inform the requester the reason for refusal and appeal rights.

6.2.4.2.7. Appeal Procedures. Individuals may appeal to the appellate authority, the Oversight and Compliance Director, within 60 calendar days after receiving a denial letter.

6.2.4.2.7.1. The Privacy Act Program Manager 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, Civil Liberties, and Transparency Division (DPCLTD), FOIA Appeals, Mailbox #24, and Alexandria, VA 22350-1700.

6.2.4.2.7.2. If the denial authority reverses an earlier denial and grants access, notify the requester immediately.

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

6.2.5. Computer Matching. Computer matching programs electronically compare records from two or more automated systems. The automated systems could be DoD, another Federal agency, or a state or other local government.

6.2.5.1. The Privacy Act applies to matching programs that use records from:

6.2.5.1.1. Federal personnel or payroll systems and Federal benefit programs where matching determines Federal benefit eligibility.

6.2.5.1.2. Checks on compliance with benefit program requirements.

6.2.5.1.3. Recovers improper payments or delinquent debts from current or former beneficiaries.

6.2.5.2. Proposed matches that could result in an adverse action against a Federal employee must meet the following requirements:

6.2.5.2.1. A written agreement between participants.

6.2.5.2.2. Approval of the Defense Data Integrity Board.

6.2.5.2.3. Matching notice published in Federal Register before matching begins.

6.2.5.2.4. Full investigation and due process enforced.

6.2.5.2.5. Act on the information, as necessary. Reference DoD 5400.11-R, Chapter 11, Computer Matching Program Procedures. (NOTE: Allow 180 days for processing requests for a new matching program.)

6.2.5.3. 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 before participating in a matching program.

6.3. PUBLISH A SYSTEMS OF RECORDS NOTICE. 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 SORN published in the Federal Register that covers the information collection. A SORN is a description of who, what, where, and why of a Privacy Act SOR; including the process for individuals to access or contest the information being held in the system. USTRANSCOM is required to publish notices in the Federal Register of new, changed, and deleted systems to inform the public of the records USTRANSCOM plans to keep and to give them an opportunity to comment within 30 days. No collection of data (paper based or electronic) can start until this step is completed.

6.3.1. The Process of Publishing a SORN. A new or altered SORN requires approval from the Office of Management and Budget (OMB) and both houses of Congress per the Paperwork Reduction Act of 1995 (PRA) by completing an Information Collection Request (ICR). This will ensure USTRANSCOM is collecting and managing information “in order to promote openness, reduce burdens on the public, increase program efficiency and effectiveness and improve the integrity, quality, and utility of information to all users within and outside of government,” referenced in OMB Memorandum, “Information Collection under the Paperwork Reduction Act,” dated 7 April 2010.

6.3.1.1. An ICR must describe the information to be collected, the reason the information is needed, and an estimate of the time and cost for the public to answer the request. Submit the ICR and supporting documentation to OMB for approval at least 40 days prior to the operation of the new or altered system. Once ICR is approved, a control number will be issued.

6.3.1.2. The ICR and the SORN can be done simultaneously. A SORN sample is located at Attachment 4. The specific elements required in this notice can be found under DoD 5400.11-R, Section C6.3.

6.3.1.3. Submit the SORN to DPCLTD in the Federal Register Format. DPCLTD will transmit the SORN to the Federal Register for publication. The public is allowed 30 days to comment on any proposed routine uses before any disclosures are made.

6.3.1.4. Next, USTRANSCOM will submit the OMB Form 83-I along with supporting statement part A to OMB. This form is located at: <https://www.whitehouse.gov/sites/default/files/omb/inforeg/83i-fill.pdf>. Once all steps are completed the collection of data (paper based or electronic) can start.

6.3.1.5. 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.”

6.4. PRIVACY ACT COMPLAINTS AND VIOLATIONS. The Privacy Act of 1974 establishes provisions that all government agencies must adhere to. It is USTRANSCOM's duty to follow these provisions, which have been laid out in USTRANSCOM's Policy and Responsibilities. If not, an individual may seek relief through administrative channels or file a civil suit.

6.4.1. Filing a Complaint. Any individual with a complaint concerning any right granted in this instruction can seek relief by filing a complaint with the Privacy Act Program Manager. Complaints can be submitted at <http://www.ustranscom.mil/foia/>.

6.4.1.1. After a written complaint is submitted, a formal investigation is launched, if the Privacy Act allegation is warranted.

6.4.1.2. If determined an USTRANSCOM employee has failed to notify an individual of a SOR being maintained on them, allowed unauthorized access, and/or failed to have a SORN published in the Federal Register; criminal penalties may apply.

6.4.2. A civil suit can be filed against USTRANSCOM, if an individual believes their rights have been violated. If successful, damages may be awarded.

7. ROLES. USTRANSCOM's Privacy Act Program has essential personnel with vital roles established in order to uphold the policy and responsibilities named in this instruction.

7.1. USTRANSCOM PRIVACY ACT PROGRAM MANAGER. The Privacy Act Program Manager serves as the subject matter expert (SME) of the Privacy Act Program. The Program Manager is responsible for ensuring USTRANSCOM is limiting the collection of personal information, informing individuals of the purpose and use of information, and publishing a SORN. The Privacy Act Program Manager is in charge of the following:

7.1.1. Submitting the DoD SSN Justification Memorandum and Form. See section 6.1.3., of this instruction for more information.

7.1.2. Training USTRANSCOM Personnel on Handling Personal Information. The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any SOR. More specialized training is needed for personnel who may be expected to deal with the news media or the public.

7.1.2.1. Periodic training will be directed by the Privacy Act Program Manager as needed. Updated information pertaining to the handling of PII will be posted on the TCJA-FO SharePoint site: <https://ustranscom.eim.amc.af.mil/sites/tcja/tcja-fo/default.aspx>.

7.1.3. Reviewing PAS. See section 6.2.1., of this instruction for more information.

7.1.4. Reviewing PIA. See section 6.2.2., of this instruction for more information.

7.1.5. Reporting Privacy Breaches. PII breaches need to be reported within one hour of discovery/detection to the United States Computer Emergency Readiness Team (US-CERT) at <https://www.us-cert.gov/>. US-CERT will use this information to notify other agencies and provides technical assistances if any DoD IT system has been compromised.

7.1.5.1. If the PII breach involves government authorized credit cards; OMB requires that issuing banks be notified.

7.1.5.2. After reporting the PII breach to US-CERT, a generated incident number will be issued to be used on the DD Form 2959, *Breach of PII Report*. The Privacy Act Program Manager will determine the point of contact for further information on the DD Form 2959 based on availability to information needed on the incident. The DD Form 2959 must be reviewed by the Component Senior Official of Privacy or designee before being submitted to DPCLTD.

7.1.5.3. When the report is completed, send the report to DPCLTD using the Compliance and Reporting Tool (CART) at <https://dpclo.osd.mil/Default.aspx>. To access CART go to <https://dpclo.osd.mil/UserRegistration.aspx>. The DD Form 2959 must be submitted within 48 hours.

7.1.5.4. Review OMB Memorandum 16-03 dated 30 October 2015, to define if the PII breach is a “major incident” at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>. If so, the “major incident” must be reported to congress within seven days.

7.1.5.5. Notify agency officials when notifying DPCLTD and establish USTRANSCOM’s response team consisting of the Chief Information Officer, Privacy Act Program Manager, Senior Official for Privacy, and a representative from the following offices; Communications, Legislative Affairs, Public Affairs, SJA, Financial Management, Intelligence, and Human Resources.

7.1.5.5.1. If it is a joint breach, the USTRANSCOM Privacy Act Office will also notify the subordinate command’s Privacy Act Office to coordinate further actions. Additionally, USTRANSCOM’s Privacy Act program manager and the subordinate’s Privacy Act office will provide instructions to the office of primary responsibility (OPR) of the breach for collecting PII information.

7.1.5.5.2. USTRANSCOM’s response team will decide whether notification is necessary by using best judgment and assess the following five factors: Nature of the data elements breached; Number of individuals affected; Likelihood the information is accessible and usable; Likelihood the breach may lead to harm; Ability of the USTRANSCOM to mitigate the risk of harm.

7.1.5.5.3. If notification is determined necessary, the response team will decide on what method to use to notify affected individuals. Review OMB M-07-16, Attachment 3, External Breach Notification, for options.

7.1.5.5.3.1. The notification shall be made as soon as all affected individual’s identities have been ascertained and no later than 10 working days from ascertained.

7.1.6. Reporting Privacy Act Complaints and Violations. See section 6.4., of this instruction for more information.

7.1.7. Verifying and Routing Privacy Act Requests. See section 6.2.4., of this instruction for more information.

7.1.7.1. 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.

7.1.7.1.1 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.

7.1.7.1.2. Document reasons for untimely responses.

7.1.8. Publishing a SORN. See section 6.3., of this instruction for more information.

7.1.9. Reviewing and Updating Instructions. USTRANSCOM I33-35 will be reviewed annually and updated when needed.

7.1.10. Preparing reports. The annual Federal Information Security Management Act (FISMA) report is usually due by the end of the fiscal year (FY). This report requires USTRANSCOM to review and update their progress on privacy procedures and practices. However, FISMA elements are subject to change. The FISMA report will be sent to DPCLTD for inclusion in their report.

7.1.11. Documenting Privacy Act Inspections. Official reports will document the findings of the inspectors, such as, deficiencies, irregularities, significant problems, and remedial actions taken.

7.2. SENIOR COMPONENT OFFICIAL FOR PRIVACY. USTRANSCOM has designated the SJA as the Senior Component Official for Privacy. The Senior Component Official for Privacy is responsible and accountable for the implementation of information privacy protections, including compliance with federal laws, regulations, and polices relating to the Privacy Act and other federally mandated information privacy policies.

7.2.1. Oversees policies and procedures. Ensures policies are comprehensive and up-to-date. Implements new or revised procedures into the program.

7.2.2. Certifies employees and contractors are receiving appropriate training and education on privacy laws, regulations, policies, and procedures on handling PII.

7.2.3. Assists in policy making for proposed legislative, regulatory, and other policy proposals associated with PII collection, use, sharing, and disclosure.

7.3. SYSTEM MANAGERS. System Managers are the officials who are responsible for managing a SOR, including policies and procedures to operate and safeguard the information contained. Systems Managers will:

7.3.1. Decide the need for and content of systems.

7.3.2. Manage and safeguard the system.

7.3.3. Train personnel on Privacy Act requirements.

7.3.4. Protect records from unauthorized disclosure, alteration, or destruction.

7.3.5. Coordinate systems notices.

7.3.5.1. 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.

7.3.5.2. The proposed system notice will be sent to the Privacy Act Program Manager at least 120 days before implementing a new SOR. The format for the proposal is at Attachment 4.

7.3.5.3 The Privacy Act Program Manager will send notices to DPCLTD 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 the Privacy Act Program Manager for processing.

7.3.5.4. 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.

7.3.6. Prepare the litigation status sheet. The litigation status sheet is used to notify the DPCLTD when a Privacy Act Complaint is filed in a U.S. District Court against USTRANSCOM. See DoD 5400.11-R, chapter 10, section 5 for more information on the litigation status sheet.

7.3.7. Answer tasked Privacy Act requests from the Privacy Act Program Manager.

7.3.8. Cooperate with investigations of complaints or allegations.

7.3.8.1. Establish and review the facts, interview individuals as needed, determine validity of the complaint, and take appropriate corrective action.

7.3.9. Keep records of disclosures.

7.3.10. Evaluate the systems annually.

8. PURPOSE OF CIVIL LIBERTIES PROGRAM. This instruction, in accordance with DoDI 1000.29, *DoD Civil Liberties Program*, establishes policy and provides responsibilities, administrative policies and procedures for the implementation of USTRANSCOM Civil Liberties Program.

9. APPLICABILITY. This instruction applies to all USTRANSCOM directorates/staff offices, joint task force headquarters, and other assigned activities and associated units under the support or control of USTRANSCOM.

10. DEFINITION. Civil Liberties. The fundamental freedoms of a citizen to exercise customary rights protected by the Constitution of the United States.

11. POLICY. It is USTRANSCOM policy to protect the privacy and civil liberties of military members and civilian employees, to the greatest extent possible, consistent with its operational requirements.

11.1. Ensure no information is maintained on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, and religion, except when:

11.1.1. Specifically authorized by statute;

11.1.2. Expressly authorized by the individual, group of individuals, or association on whom the record is maintained; or

11.1.3. The record is pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counter intelligence activity.

12. RESPONSIBILITIES. USTRANSCOM will have adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege USTRANSCOM has violated their privacy or civil liberties. The Civil Liberties Program Manager will ensure the following:

12.1. Place Civil Liberties Program information on the FOIA SharePoint at <https://ustranscom.eim.amc.af.mil/sites/tcja/tcja-fo/default.aspx>.

12.2. Establish procedures for the investigation of complaints from individuals who allege USTRANSCOM violated their privacy or civil liberties.

12.3. Coordinate privacy and civil liberties activities with USTRANSCOM Inspector General's (IG) office and the 375th Air Mobility Wing's (AMW) Equal Opportunity (EO) office to avoid duplication of effort.

12.4. Submit reports as directed by the Defense Privacy and Civil Liberties Office:

12.4.1. Semiannual from first half: October 1 to March 31; second half: April 1 to October 1.

12.5. Ensure all USTRANSCOM employees and members are trained regarding the protection of privacy and civil liberties.

12.6. Consider privacy and civil liberties when proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to the USTRANSCOM mission.

12.7. Periodically investigate and review USTRANSCOM actions, procedures, guidelines, and related laws to their implementation to ensure USTRANSCOM is considering appropriately privacy and civil liberties.

12.8. USTRANSCOM IG and Judge Advocate (JA) including the 375th AMW EO will refer and report complaints that may be civil liberties related to the Civil Liberties Program Manager for review/resolution. The Civil Liberties Program Manager will determine if the complaint is valid and then refer to the most appropriate office for investigation.

12.9. Complaint Processing. Written complaints will be addressed to: USTRANSCOM/TCJA-FO, ATTN: Civil Liberties POC, 508 Scott Drive, Scott AFB, IL 62225-5357 or electronically at <https://ww2.ustranscom.mil/foia.cfm>.

12.9.1. The complaint will be reviewed to determine validity.

12.9.2. A valid complaint must contain:

12.9.2.1. The civil liberties violation

12.9.2.2. When the violation occurred or whether on-going

12.9.2.3. Specific location

12.9.2.4. Name of individual(s) who violated member's civil liberties

12.9.2.5. Explain how situation was resolved, if resolved

12.9.3. Within five working days of receipt the complaint will be logged into the Civil Liberties Office database and acknowledged in writing to the requester by the Civil Liberties Program Manager.

12.9.3.1. USTRANSCOM Civil Liberties Program Manager will assign the complaint to the appropriate agency:

12.9.3.1.1. Inspector General (IG)

12.9.3.1.2. Equal Opportunity (EO) Office

12.9.3.1.3. Legal (JA)

12.9.3.2. Within twenty working days an initial resolution will be determined. If a resolution cannot be determined within twenty working days, the Civil Liberties Office will send interim update letters as warranted by the investigation.

13. RELEASABILITY. This instruction is approved for unlimited release. DoD components and other federal agencies may obtain copies of this instruction through controlled Internet access from the unclassified USTRANSCOM Publications Home Page at <http://www.ustranscom.mil/cmd/fpindex.cfm>.

ERIC J. WERNER
Colonel, USAF
Staff Judge Advocate

Attachments:

1. Glossary of References, Abbreviations, Acronyms, and Terms
2. Sample Privacy Act Statement (PAS)
3. Privacy Act Request Form
4. 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 5760.01A, *Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule*

OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of PII*, 22 May 07

OMB Memorandum, *Information Collection under the Paperwork Reduction Act*, dated 7 April 2010.

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 1000.29, *Department of Defense Civil Liberties Program*

Department of Defense Instruction 1000.30, *Reduction of SSN Use Within Department of Defense*

Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties 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
AMW	Air Mobility Wing
CART	Compliance and Reporting Tool
CJCSM	Chairman Joint Chiefs of Staff Manual
CIO	Chief Information Officer
CSG	Command Support Group
DoD	Department of Defense
DoDI	Department of Defense Instruction
DPCLTD	Defense Privacy, Civil Liberties, and Transparency Division
DTS	Defense Travel System

E-Government	Electronic Government
E-Mail	Electronic Mail
EO	Equal Opportunity
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FY	Fiscal Year
ICR	Information Collection Request
IDA	Initial Denial Authority
IG	Inspector General
IT	Information Technology
JA	Judge Advocate
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
SJA	Staff Judge Advocate
SME	Subject Matter Expert
SOR	System of Records
SORN	System of Records Notice
SSN	Social Security Number
TCJ3-F	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
UCMJ	Uniform Code of Military Justice
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 SOR to make the data accurate, relevant, timely, or complete.

Civil Liberties. The fundamental freedoms of a citizen to exercise customary rights protected by the Constitution of the United States.

Computer Matching. A computerized comparison of two or more automated systems of records or a SOR 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 identity 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 SOR 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.

Joint Breach: A breach consisting of loss of control, compromise, or any situation where persons other than authorized users have potential access to PII whether physical or electronic within IT systems and/or administrative processes that multiple commands manage.

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 Advisory. A statement required when soliciting individual's Social Security Number for the authentication purpose only and will not be maintained in a System of Record. The Privacy Advisory informs the individual why the information is being solicited and how it will be used.

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 SOR 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 SOR 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

Global Air Transportation Execution System (GATES)

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 8013

PRINCIPAL PURPOSE: To apply for air travel. SSN is needed for positive ID.

ROUTINE US(S): Records from this SOR may be disclosed for any of the blanket routine uses published by DoD.

DISCLOSURE IS VOLUNTARY: Disclosure of SSN is voluntary. However failure to provide the information may result in member not being accepted for travel on military aircraft.

Attachment 3

USTRANSCOM Freedom of Information Act and Privacy Act Request

1. Full Name of Requester

2. Type of records being requested:

3. Citizenship Status

4. Date of Birth and Place

5. Current Address

**An individual submitting a request under the Privacy Act of 1974 must be either "a citizen of the United States" or an "alien lawfully admitted for permanent residence," pursuant to 5 U.S.C. Section 552a(a)(2). Requests will be processed as Freedom of Information Act requests pursuant to 5 U.S.C. Section 552, rather than Privacy Act requests, for individuals who are not United States citizens or aliens lawfully admitted for permanent residence.*

You may be contacted for your **social security number if records relating to you can only be located with this identifying number.*

Please provide USTRANSCOM with two different forms of identification (i.e. passport, driver's license, copy of birth certificate, certificate of U.S. citizenship [Form N-560 or N-561], and/or certificate of naturalization [Form N-550 or N-570]), with this form. **Once notarized and completed, please e-mail form to transcom.scott.tcja.mbx.foia@mail.mil.**

----- Notarized Statement -----

Print or Type Name: _____

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that I am the person named above, and I understand that any falsification of this statement is punishable under the provisions of 18 U.S.C. Section 1001 by a fine of not more than \$10,000 or by imprisonment of not more than five years or both, and that requesting or obtaining any record(s) under false pretenses is punishable under the provisions of 5 U.S.C. 552a(i)(3) by a fine of not more than \$5,000.

Signature _____ **Date** _____

State of _____

County of _____

This instrument was signed before me on _____

by _____

Print name of signer(s)

Notary Signature

Affix seal/stamp as close to signature as possible

Attachment 4
SAMPLE OF NEW OR ALTERED SORN
IN FEDERAL REGISTER FORMAT

(Reference DoD 5400.11-R, Chapter 6 at
<http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf>)

New Systems of Records Notice

DEPARTMENT OF DEFENSE

Office of the Secretary

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD

ACTION: Notice to Add a System of Records

SUMMARY: The Office of the Secretary of Defense proposes to add a SOR to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

DATES: The changes will be effective on (insert date thirty days after publication in the Federal Register) unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to OSD Privacy Act Coordinator, Records Management Section, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301-1155.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000-0000.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address above.

The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, were submitted on January 20, 2006, to the House Committee on Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: February 1, 2006.

John Miller

Alternate OSD Federal Register Liaison Officer, Department of Defense.

NSLRB 01

System name:

The National Security Labor Relations Board (NSLRB).

System location:

National Security Labor Relations Board (NSLRB), 1401 Wilson Boulevard, Arlington, VA 22209- 2325.

Categories of individuals covered by the system:

Current and former civilian Federal Government employees who have filed unfair labor practice charges, negotiability disputes, exceptions to arbitration awards, and impasses with the National

Security Labor Relations Board (NSLRB) pursuant to the National Security Personnel System (NSPS).

Categories of records in the system:

Documents relating to the proceedings before the Board, including the name of the individual initiating NSLRB action, statements of witnesses, reports of interviews and hearings, examiner's findings and recommendations, a copy of the original decision, and related correspondence and exhibits.

Authority for maintenance of the system:

The National Defense Authorization Act for FY 2004, Pub Law 108-136, Section 1101; 5 U.S.C. 9902(m), Labor Management Relations in the Department of Defense; and 5 CFR 9901.907, National Security Labor Relations Board.

Purpose(s):

To establish a SOR that will document adjudication of unfair labor practice charges, negotiability disputes, exceptions to arbitration awards, and impasses filed with the National Security Labor Relations Board.

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, 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 The Federal Labor Relations Authority (FLRA) or the Equal Employment Opportunity Commission, when requested, for performance of functions authorized by law.

To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

To provide information to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.

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 and paper.

Retrievability:

Records will be retrieved in the system by the following identifiers: assigned case number; individual's name; labor organizations filing the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; date, month, year or filing; complaint type; and the organizational component from which the complaint arises.

Safeguards:

Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly

screened and cleared for need-to-know. Access to computerized data is restricted by passwords, which are changed periodically.

Retention and disposal:

Records are disposed of 5 years after final resolution of case.

System manager(s) and address:

Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209-2325.

Notification procedure:

Individuals seeking to determine whether this SOR contains information about themselves should address written inquiries to the Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209-2325.

Request should contain name; assigned case number; approximate case date (day, month, and year); case type; the names of the individuals and/or labor organizations filed the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; and impasses.

Record access procedures:

Individuals seeking access to records about themselves contained in this SOR should address written inquiries to the Executive Director, National Security Personnel System, Program Executive Office, 1401 Wilson Boulevard, Arlington, VA 22209-2325.

Request should contain name; assigned case number; approximate case date (day, month, and year); case type; the names of the individuals and/or labor organizations filed the unfair labor practice charges; negotiability disputes; exceptions to arbitration awards; and impasses.

Contesting record procedures:

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

Record source categories:

Individual; other officials or employees; and departmental and other records containing information pertinent to the NSLRB action.

Exemptions claimed for the system:
None.

Altered Systems of Records Notice

DEPARTMENT OF DEFENSE

Defense Logistics Agency

Privacy Act of 1974; Systems of Records

AGENCY: Defense Logistics Agency

ACTION: Notice to Alter a System of
Records

SUMMARY: The Defense Logistics Agency proposes to alter a SORN in its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

The alteration adds two routine uses, revises the purpose category, and makes other administrative changes to the system notice.

DATES: This action will be effective without further notice on (insert date thirty days after publication in the Federal Register) unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DSS-B, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060-6221.

FOR FURTHER INFORMATION CONTACT: Ms. Mary Smith at (703) 000-0000.

SUPPLEMENTARY INFORMATION: The Defense Logistics Agency notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address above.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on January 29, 2004, to the House Committee on Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: February 2, 2004.

John Miller

Alternate OSD Federal Register Liaison Officer, Department of Defense.

S253.10 DLA-G

System name:

Invention Disclosure (February 22, 1993, 58 FR 10854).

Changes:

* * * * *

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 numbers; 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) as 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 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 of Counsel are destroyed 26 years after file is closed. Records maintained by field level Offices of Counsel where patent applications are not prepared are destroyed 7 years after closure."

* * * * *

Record 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:

Invention Disclosure.

System location:

Office of the General Counsel, HQ DLA-DG, 8725 John J. Kingman Road, Stop 2533, Fort Belvoir, VA 22060-6221, and the offices of counsel of the DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Categories of individuals covered by the system:

Employees and military personnel assigned to DLA who have submitted invention disclosures to DLA.

Categories of records in the system:

Inventor's name, Social Security Number, address, and telephone numbers; 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:

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) as amended by E.O. 10930.

Purpose(s):

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 purposes of such uses:

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 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.

Information may be referred to other government agencies or to non-government agencies or to non-government personnel (including contractors or prospective contractors) having an identified interest in a particular invention and the Government's rights therein.

The DoD "Blanket Routine Uses" set forth at the beginning of DLA'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:

Filed by names of inventors.

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:

Records maintain by the HQ and field Offices of Counsel are destroyed 26 years after file is closed. Records maintained by field level Offices of Counsel where patent applications are not prepared are destroyed 7 years after closure.

System manager(s) and address:

Office of the General Counsel, Headquarters, Defense Logistics Agency, ATTN: DG, 8725 John J. Kingman Road, Stop 2533, Fort Belvoir, VA 22060-6221.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Privacy Officer, Headquarters, Defense Logistics Agency, ATTN: DSS-B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060-6221, or the Privacy Officers at DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Record access procedures:

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Privacy Officer, Headquarters, Defense Logistics Agency, ATTN: DSS-B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060-6221, or the Privacy Officers at the DLA field activities. Official mailing addresses are published as an appendix to DLA's compilation of systems of records notices.

Individuals should provide information that contains full name, current address and telephone numbers of requester.

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

Contesting record procedures:

The DLA rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 323, or may be obtained from the Privacy Act Officer, Headquarters, Defense Logistics Agency, ATTN: DSS-B, 8725 John J. Kingman Road, Stop 6220, Fort Belvoir, VA 22060-6221.

Record source categories:

Inventors, reviewers, evaluators, officials of U.S. and foreign patent offices, and other persons having a direct interest in the file.

Exemptions claimed for the system:

None.