BY ORDER OF THE COMMANDER
UNITED STATES TRANSPORTATION COMMAND

USTRANSCOM INSTRUCTION 33-11
13 OCTOBER 2011

Communications and Information

UNITED STATES TRANSPORTATION COMMAND PRIVACY IMPACT ASSESSMENT

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: TCJ6-IM
Supersedes: USTRANSCOMI 33-11, 7 May 2008

Approved By: TCJ6 (Brig Gen Gregory J. Touhill, USAF)
Pages: 11
Distribution: e-Publishing

The purpose of this instruction is to ensure United States Transportation Command (USTRANSCOM) applies Fair Information Practice Principles on collected Personally Identifiable Information (PII) in USTRANSCOM-owned systems. This instruction establishes standards and procedures to follow when implementing the Privacy Impact Assessment (PIA) requirements mandated in Section 208 of the Electronic Government Act of 2002. This instruction applies to USTRANSCOM, its Transportaiton Component Commands, and to systems funded by USTRANSCOM. Refer recommended changes and questions about this publication to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this instruction are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

SUMMARY OF REVISIONS

This instruction has been updated for revised content. Revised and eliminated some attachments.

1. References and Supporting Information. References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. Policy. USTRANSCOM will adhere to the PIA requirements prescribed in the Office of Management and Budget Memorandum 03-22, dated 26 September 2003,*Guidance for Implementing the Privacy Provision of the E-Governement Act of 2002,* in addition to Department of Defense (DOD) specific requirements outlined in the DOD Guidance section of Attachment 1, References and Acronyms. These requirements extend to all unclassified USTRANSCOM systems that collect, store, retrieve, manage, transmit, or process PII. Note**:** Program Managers may request a Statement of Exemption (Attachment 2) from Chief Information Officer and Investment Management Branch (TCJ6-IM) for systems that were procured/developed before 26 September 2003, have not implemented new capability or enhanced existing capability that requires collection of identifiable information, and have a termination date within 12 months. Program Management Offices receiving the Statement of Exemption should consider exercising Fair Information Practice Principles.

2.1. Fair Information Practice Principles: Under the Privacy Act of 1974, United States citizens and certain other persons have specific guarantees commonly referred to as the Fair Information Practice Principles. The five core principles are:

2.1.1. Notice/Awareness. Individuals should be informed of an entity's information handling practices; and the collection, use, disclosure, and retention of PII should be limited to that which is consistent with stated purposes.

2.1.2. Choice/Consent. To the extent possible, options should be provided to individuals regarding the collection and use of their PII.

2.1.3. Access/Participation. Individuals should have the ability to view their information and/or contest the data accuracy and completeness.

2.1.4. Integrity/Security. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

2.1.5. Enforcement/Redress. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are self-regulation, the Privacy Act itself, and/or regulatory schemes enforceable through civil and criminal sanctions.

3. PIA Goals. To ensure that systems with new or modified electronic PII are evaluated for privacy risks and designed to meet Privacy Act life cycle management requirements (collection, use, retention, processing, disclosure, and destruction), and to ensure that appropriate privacy protection measures are in place for the systems that collect, store, retrieve, manage, transmit, or process PII.

4. Roles and Responsibilities.

4.1. Program Managers (PM) will:

4.1.1. Ensure systems that collect, store, retrieve, transmit, or process personal information comply with this instruction and DODD 5400.11, *DOD Privacy Program*, as well as DOD 5400.11-R, *DOD Privacy Program*.

4.1.2. Conduct or update the PIAs, as necessary, when systems create or change privacy risks (DD Form 2930, *Privacy Impact Assessment*). Process PIA as outlined in the PIA Flowchart (Attachment 4).

4.1.3. Implement PIA controls identified in the Information Assurance (IA) Security Controls found in DODI 8500.2, *Information Assurance Implementation* (Attachment 3).

4.1.4. Register the system in USTRANSCOM Information Tool Suite (ITS) and submit data models and system design documents to ustc-ciosupport@ustranscom.mil. Systems which have achieved operational capability, i.e., have passed Milestone C, must also submit security certification and accreditation artifacts.

4.1.5. Complete DD Form 2930, *Privacy Impact Assessment*, including the preparing official information and signature and forward to ustc-ciosupport@ustranscom.mil for validation and approval. Ensure the answers supplied in section I & II are publicly releasable**.**

4.1.6. Ensure all security incidents involving PII are reported to the Component Information Assurance Manager at the time of discovery. Incidents include electronic, physical, suspected, and confirmed breaches.

4.2. Chief Information Officer (CIO) Support, TCJ6-IM, will:

4.2.1. Ensure PMs conduct a PIA before developing or procuring a system that will collect, store, retrieve, manage, transmit, or process PII; or before modifying processes for handling PII in an existing system.

4.2.2. Assist PMs with completion of a PIA package.

4.2.3. Ensure PIAs are completed prior to Interim Authority to Operate or Authority to Operate is granted.

4.2.4. Verify that PMs have updated their PIA Questionnaires and implemented PIA controls to reflect any changed information, collection authorities, business processes, or other factors affecting the handling of PII.

4.2.5. Ensure the PIAs adhere to the PIA requirements outlined in DODI 5400.16, *Privacy Impact Assessment.*

4.2.6. Review documents noted in paragraph 4.1.5. to verify and validate presence/absence of PII and that any PII is protected in accordance with DODI 5400.16.

4.2.7. Assess PM answers to DD Form 2930 and provide feedback for improvements. Coordinate the PIA Signature section of DD Form 2930 within USTRANSCOM for completion. Ensure signatures are accomplished using DOD-approved certificates.

4.2.8. Submit sections 1 and 2 of the CIO-approved PIA to the USTRANSCOM Gate Keeper for posting on the USTRANSCOM public website and Freedom of Information Act Service Center Reading Room. This satisfies requirements to make the PIA available for public review.

4.2.9. E-mail the web Uniform Resource Locator generated by the Gate Keeper to DOD CIO (pia@osd.mil) and courtesy copy the PM Office.

4.2.10. Periodically, ensure PIA data in the DOD Information Technology Portfolio Repository is up-to-date and consistent with ITS.

4.2.11. Report USTRANSCOM's overall PIA status to the DOD CIO via e-mail, as required.

4.2.12. Initiate a Statement of Exemption (Attachment 2) when PMs make valid requests.

4.3. Senior Information Assurance Officer shall:

4.3.1. Review and coordinate proposed PIAs to ensure compliance with DOD and USTRANSCOM information assurance policies.

4.3.2. Review PM's PIA questionnaires to verify and ensure consistency with system information already provided for other reporting requirements, e.g., Exhibit 300 and technical assessment input in ITS.

4.3.3. Act as the Subject Matter Expert for PIA security-related issues in support of PMs and the CIO Support Staff.

4.3.4. Verify the security environment described in the questionnaire is consistent with the environment described in the system certification and accreditation documentation, i.e., ensure systems employ adequate and sufficient PIA security controls as identified in IA Security Controls.

4.3.5. Provide a memorandum to TCJ6-IM stating all findings with rationale, as necessary.

4.3.6. Function as the CIO liaison to United States-Computer Emergency Readiness Team for security incidents involving PII.

4.4. Privacy Act Officer shall:

4.4.1. Review and coordinate proposed PIAs to confirm all privacy concerns have been identified.

4.4.2. Advise TCJ6-IM as needed.

4.5. Staff Judge Advocate shall:

4.5.1. Review and coordinate proposed PIAs to ensure compliance with the existing laws and regulations.

4.5.2. Provide a memorandum to TCJ6-IM stating all findings with rationale, as necessary.

4.6. CIO will:

4.6.1. Serve as the USTRANSCOM PIA Reviewing/Approving Official

4.6.2. Provide direction and feedback to TCJ6-IM, as needed.

4.6.3. Provide PIA information to the DOD CIO, as requested.

5. Exception: A PIA may not be required when:

5.1. The system is a National Security System.

5.2. The system does not collect, store, retrieve, manage, transmit, or process PII.

5.3. The system meets requirements for a Statement of Exception (Attachment 2). Request a Statement of Exemption from TCJ6-IM when a system meets stated criteria.

6. Adopted Form: DD Form 2930, *Privacy Impact Assessment*.

GREGORY J. TOUHILL
Brigadier General, USAF
Director, Command, Control, Communications
and Computer Systems

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Section 1-References:

President's Memorandum for the Head of Executive Departments and Agencies, 14 May 1998, *Privacy and PII in Federal records*
Public Law 107-347, Section 208, *Privacy Provisions of E-Government Act of 2002*
Office of Management and Budget Memorandum 03-22, 26 September 2003, *OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002*
OMB Circular A-11
DODD 5400.11, *DOD Privacy Program*
DOD 5400.11-R, *DOD Privacy Program*
DODD 5400.16, *Privacy Impact Assessment*
DODI 8500.2, *Information Assurance Implementation*
USTRANSCOM Instruction 33-35, *USTRANSCOM Privacy Act Program*

Section 2 -Acronyms:

CIO - Chief Information Officer
DOD - Department of Defense
IA – Information Assurance
ITS - Information Tool Suite
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
PM - Program Manager
TCJ6-IM - Chief Information Officer and Investment Management Branch
USTRANSCOM - United States Transportation Command

Section 3 – TERMS AND DEFINITIONS:

Budget System Identification Number (BIN): This number is used by the program managers when they budget for the system.

Exhibit 300: Also known as "Capital Asset Plan and Business Case" is for the Federal Government to effectively manage its portfolio of capital assets to ensure scarce public resources are wisely invested. Capital programming integrates the planning, acquisition, and management of capital assets into the budget decision-making process, and is intended to assist agencies in improving asset management and in complying with the results-oriented requirements (Source: OMB Circular A-11).

IT Investment Unique Identifier: A system's submission number to the Office of Management and Budget.

National Security Systems: National Security System (NSS) is any information system

(including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:

* Involves intelligence activities
* Involves crypto logic activities related to national security
* Involves command and control of military forces
* Involves equipment that is an integral part of a weapon or weapon system
* Is critical to the direct fulfillment of military or intelligence missions
* Is protected at all times by procedures established for information that has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: Title 44, U.S. Code Section 3542 (b)(2), Federal Information Security Management Act (FISMA), Title III, Public Law 107-347.

Office of Management and Budget Information Collection Requirement Number and Expiration Date: A number and expiration date is issued by Office of Management and Budget when System of Records Notice is received.

Privacy Impact Assessment (PIA) Questionnaire: Set of questions addressing when privacy protection measures are in place for systems that store/process PII.

Privacy Act Statement: Is used when an individual is requested to furnish personal information about himself or herself for inclusion in a system of records. A Privacy Act Statement is required regardless of the medium used to collect the information. If the information requested will not be included in a Privacy Act system of records, a Privacy Act Statement is not required.

Privacy Advisory: Is used if a person is asked to provide personal information and that info will not be maintained in a Privacy Act system of records. See section 7 of the Privacy Act. For additional information refer to Section 12.2 within the DOD Web Policy document at http://www.defense.gov/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.aspx

Privacy Impact Assessment (PIA): Is an analysis of how information is handled: to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of collecting, maintaining, and disseminating personally identifiable information in an electronic information system, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Personally Identifiable Information (PII): Is information about an individual that identifies, relates, or is unique to, or describes their personal information (e.g., a social security number, age, marital status, race, home phone numbers; and other demographic, biometric, personnel, medical, and financial information, etc.). Such information is also known as Personally Identifiable Information (e.g., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other Personally Identifiable

Information which is linked or linkable to a specified individual).

System Identification Number: A System Identification Number is a DOD Information Technology Portfolio Repository registration number. It is posted by the system description in ITS.

System of Records Notice (SORN): A SORN is required if the system contains information about citizens or lawful permanent residents that is retrieved by name or other unique identifier. When completing the Privacy Impact Assessment Questionnaire (Attachment 4), refer to the system's Privacy Act System of Record Notice, if applicable, for standardized information. If a major change occurs to the system, the System of Record Notice must be updated.

Attachment 2

STATEMENT OF EXEMPTION

MEMORANDUM FOR THE **SYSTEM NAME** PROGRAM MANAGEMENT OFFICE

FROM: UNITED STATES TRANSPORTATION COMMAND (USTRANSCOM)
CHIEF INFORMATION OFFICER (CIO)

SUBJECT: Statement of Exemption on Privacy Impact Assessment (PIA) Compliance for **System Name**

1. **System Name** was procured/developed before 26 September 2003 and has not implemented new capability or enhanced existing capability that requires collection of identifiable information. In addition, **System Name** is scheduled to terminate **Date** (must be within 12 months). **System Name** is exempt from PIA Compliance requirements. However, **System Name** should consider exercising the Fair Information Practice Principles stated in the USTRANSCOM Instruction 33-11 until **System Name** is permanently terminated.

2. Point of contact for this **System Name** Statement of Exemption on PIA Compliance is the TCJ6-IM, Defense Switched Network 779-1317, ustc-ciosupport@ustranscom.mil.

CIO, USTRANSCOM

cc:
TCJ6-IM

Attachment 3

Privacy Impact Assessment CONTROLS

The Program Manager (PM) is responsible for implementing the following PIA security controls:

1. When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

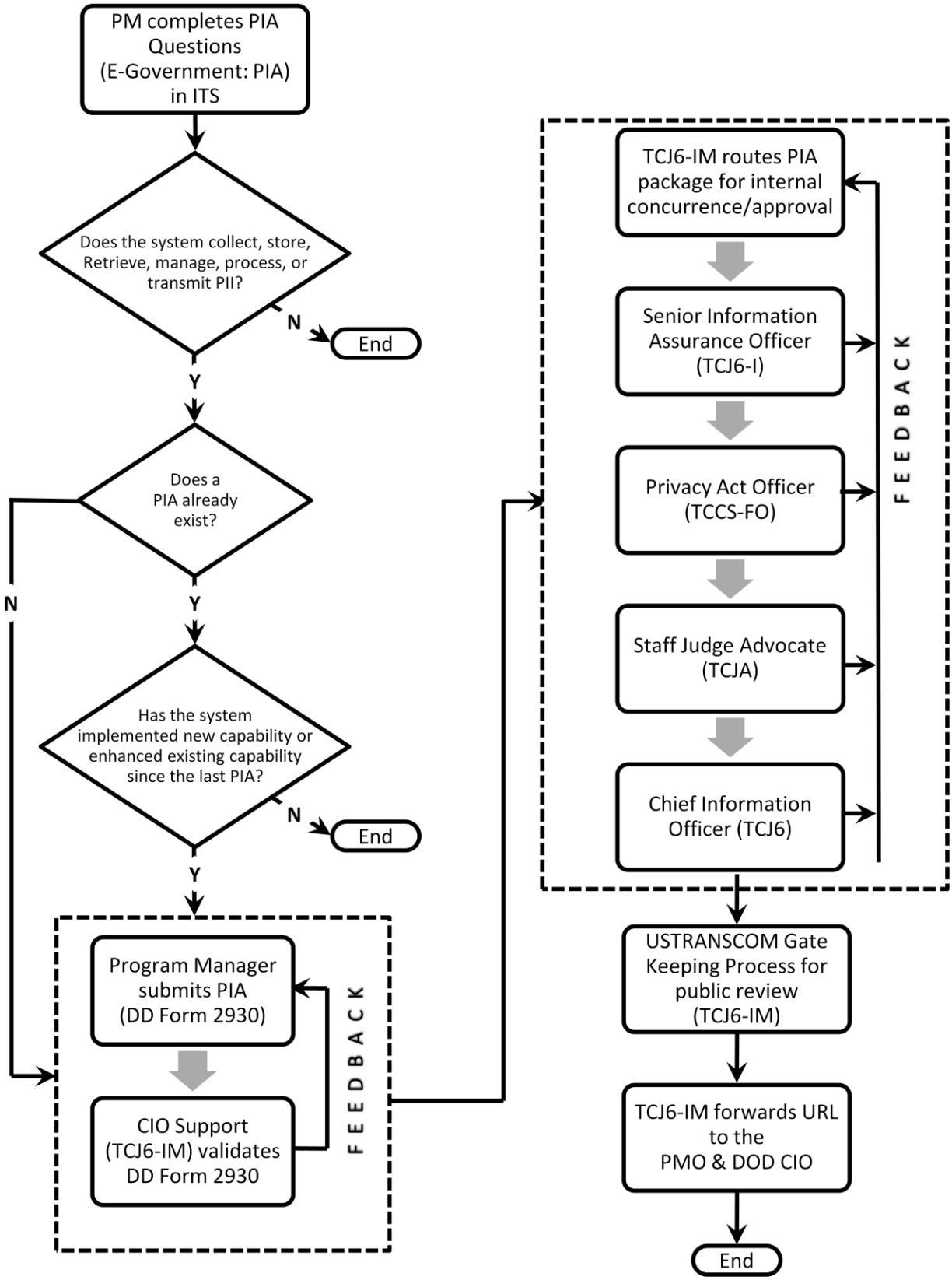
2. The information system prevents unauthorized and unintended information transfer via shared system resources.

3. The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

4. The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (i.e., security administrators).

5. The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

6. The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

7. The information system generates audit records (i.e., number of success/fail log attempts by users).

Attachment 4