BY ORDER OF THE COMMANDER
UNITED STATES TRANSPORTATION COMMAND

USTRANSCOM INSTRUCTION 33-11
22 FEBRUARY 2019

Communications and Information

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-XS
Supersedes: USTRANSCOMI 33-11, 6 January 2015

Pages: 8
Distribution: e-Publishing

This instruction establishes standards and procedures to implement Privacy Impact Assessment (PIA) requirements as mandated in Section 208 of the Electronic Government Act of 2002 and DOD Instruction (DODI) 5400.16, *DOD Privacy Impact Assessment (PIA) Guidance*. This instruction applies to USTRANSCOM, its Transportation Component Commands, subordinate commands, and to systems primarily 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, *Records Management Program*.

SUMMARY OF REVISIONS

This instruction has been updated to require the completion of a DD Form 2930, *Privacy Impact Assessment*, by all systems to document whether the privacy requirements do, or do not, apply to system. Additionally, the roles and responsibilities and process flowcharts have been updated in accordance with Office of Management and Budget (OMB) Circular No. A-130, DODI 5400.16, and USTRANSCOM processes.

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

2. Policy. All USTRANSCOM components, subordinate commands, and funded programs will adhere to the PIA requirements prescribed in OMB Circular No. A-130, DODI 5400.16, and the guidance in this instruction.

3. Purpose. To identify information technology (IT) systems and electronic collections (hereafter referred to simply as "systems") that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII) and ensure they:

a. Conform to all applicable legal, regulatory, and policy requirements regarding privacy.

b. Meet Privacy Act life cycle management requirements, i.e., that they are maintained,

used, preserved, and disposed of in accordance with National Archives and Records Administration, DODI 5015.02, and USTRANSCOM approved records schedules.

4. Roles and Responsibilities.

4.1. Program Managers will:

4.1.1. Complete a DD Form 2930 to determine whether this does or does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. In the case where no PII is collected, or the PII is determined to be releasable, the form will serve as conclusive determination that privacy requirements do not apply to the system.

4.1.2. Ensure systems that do create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII comply with this instruction, DODD 5400.11, DOD 5400.11-R, OMB Circular No. A-130, and DODI 5400.16.

4.1.3. Complete a new DD Form 2930 within 3 years of a previous assessment's approval date or sooner when a significant system change or a change in privacy or security posture occurs.

4.1.4. Register the system in the System Information application of the USTRANSCOM Information Tool Suite. All data pertaining to a system's privacy posture is maintained in Information Tool Suite for internal USTRANSCOM use and/or reporting to the DOD Chief Information Officer (CIO).

4.1.5. Forward completed DD Form 2930 to the TCJ6 CIO Support mailbox (transcom.scott.tcj6.mbx.cio-support@mail.mil) for review, staffing, and coordination for approval.

4.1.6. Ensure all security incidents involving PII are reported in accordance with the procedures provided in USTRANSCOMI 33-35, *Privacy Act and Civil Liberties Program*.

4.2. Security Policy and Compliance Branch (TCJ6-XS) will:

4.2.1. Assist program office representatives with completion of the DD Form 2930.

4.2.2. Review submitted DD Form 2930 for completeness and accuracy.

4.2.3. Submit DD Form 2930 signed by the USTRANSCOM CIO to the USTRANSCOM Privacy Office (TCJA-FO).

4.2.4. Ensure PIA data in Information Tool Suite is up-to-date.

4.3. Staff Judge Advocate (TCJA) will:

4.3.1. Serve as the subject matter expert for all legal issues related to privacy impact assessments.

4.3.2. Ensure submitted DD Form 2930 is compliant with applicable laws and regulations.

4.3.3. Sign DD Form 2930 after all legal requirements are satisfactorily addressed.

4.4. Privacy Act Officer (TCJA-FO) will:

4.4.1. Serve as the subject matter expert for Privacy Act issues.

4.4.2. Ensure the risks and threat mitigation efforts described in the submitted DD Form 2930 comply with all Federal, DOD, and USTRANSCOM privacy policies.

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

4.4.4. Sign DD Form 2930 after all privacy act issues are satisfactorily addressed.

4.4.5. Submit Section 1 of DD Form 2930 signed by the USTRANSCOM CIO to the Gate Keeper for processing and posting to the USTRANSCOM Freedom of Information Act website.

4.4.6. Submit an electronic copy of each approved PIA to the DOD CIO per instructions in DODI 5400.16.

4.5. Records Manager (TCJ6-SC) will:

4.5.1. Serve as the subject matter expert for all National Archives and Records Administration approved records schedule requirements associated with privacy impact assessments.

4.5.2. Ensure submitted DD Form 2930 contains accurate information on National Archives and Records Administration Job Number or General Records Schedule Authority, SF-115 submission date (if pending) retention instructions.

4.5.3. Obtain OMB control number, if required, pursuant to DODM 8910.01, Volume 2, *DOD Information Collections Manual: Procedures for DOD Public Information Collections.*

4.5.4. Sign DD Form 2930 after all records management requirements are satisfactorily addressed.

4.6. Chief Information Security Officer (TCJ6-X*)* will:

4.6.1. Serve as or designate a subject matter expert for Cybersecurity issues associated with privacy impact assessments.

4.6.2. Ensure submitted DD Form 2930 complies with all applicable cybersecurity policies.

4.6.3. Sign DD Form 2930 after all cybersecurity requirements are satisfactorily addressed.

4.7. Senior Component Official for Privacy will:

4.7.1. Develop, implement, and maintain an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding PII.

4.7.2. Ensure submitted DD Form 2930 complies with all applicable statutes, regulations, and procedures regarding privacy policy and managing privacy risks at the agency.

4.7.3. Sign DD Form 2930 when all privacy policy and risk management requirements are satisfactorily addressed.

4.8. USTRANSCOM CIO (TCJ6) will:

4.8.1. Serve as the USTRANSCOM PIA reviewing/approving official.

4.8.2. Sign DD Form 2930 after all legal, privacy, records management, and cybersecurity requirements are satisfactorily addressed.

JOHN C. FLOURNOY, JR.
Major General, USAF
Chief of Staff

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Section A – References

E-Government Act of 2002 - Section 208, *Privacy Provisions*
OMB Circular No. A-130, *Managing Information as a Strategic Resource*
DODI 5015.02, *DOD Records Management*
DODD 5400.11, *DOD Privacy Program*
DOD 5400.11-R, *DOD Privacy Program*
DODD 5400.16, DOD *Privacy Impact Assessment (PIA) Guidance*
DODM 8910.01, Volume 2, *DOD Information Collections Manual: Procedures for DOD Public Information Collections.*
USTRANSCOMI 33-35, *Privacy Act and Civil Liberties Program*

Section B – Abbreviations and Acronyms

CIO – Chief Information Officer
DOD – Department of Defense
DODD – DOD Directive
DODI – DOD Instruction
OMB – Office of Management and Budget
PIA – Privacy Impact Assessment
PII – Personally Identifiable Information
USTRANSCOM – United States Transportation Command

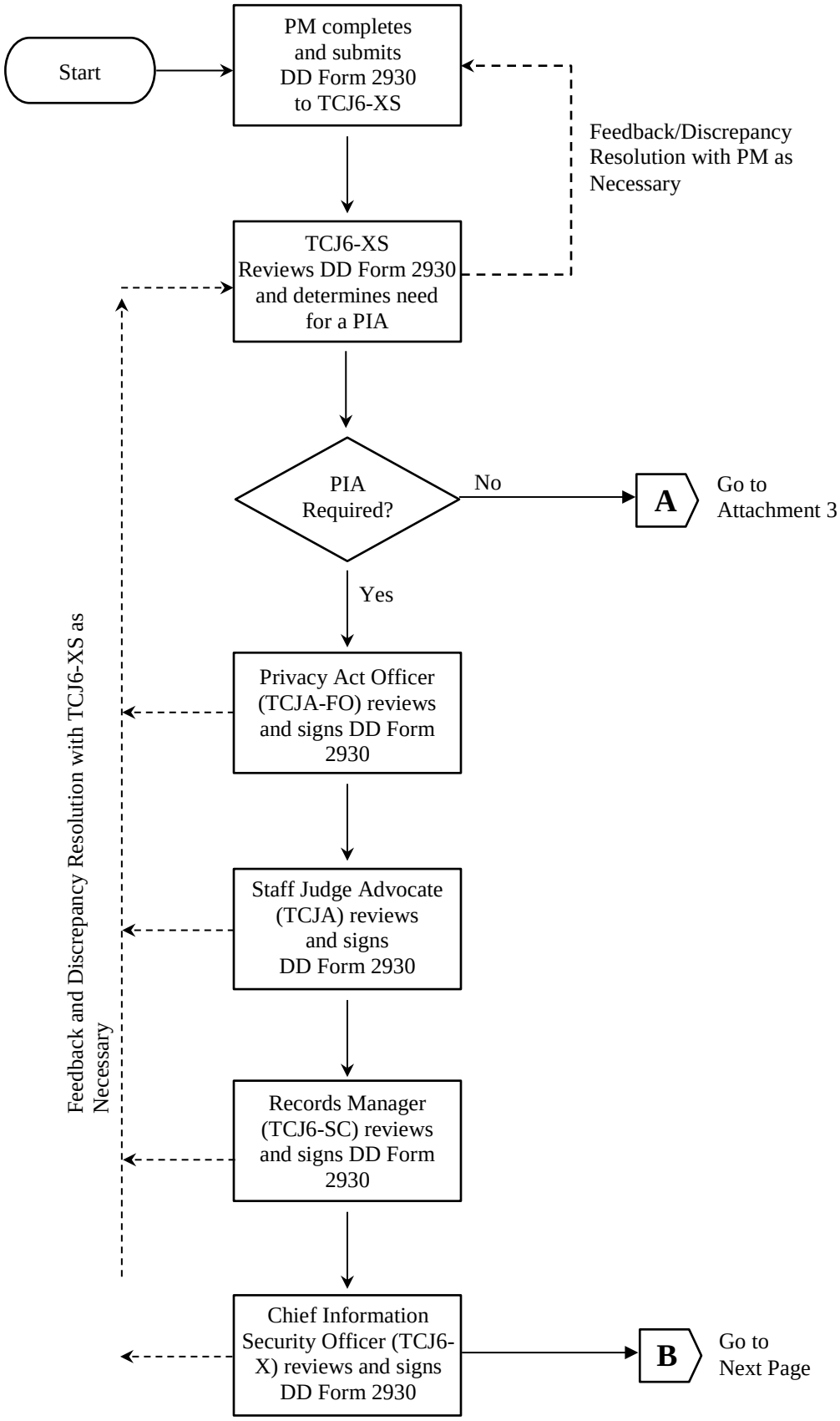
Section C – Terms

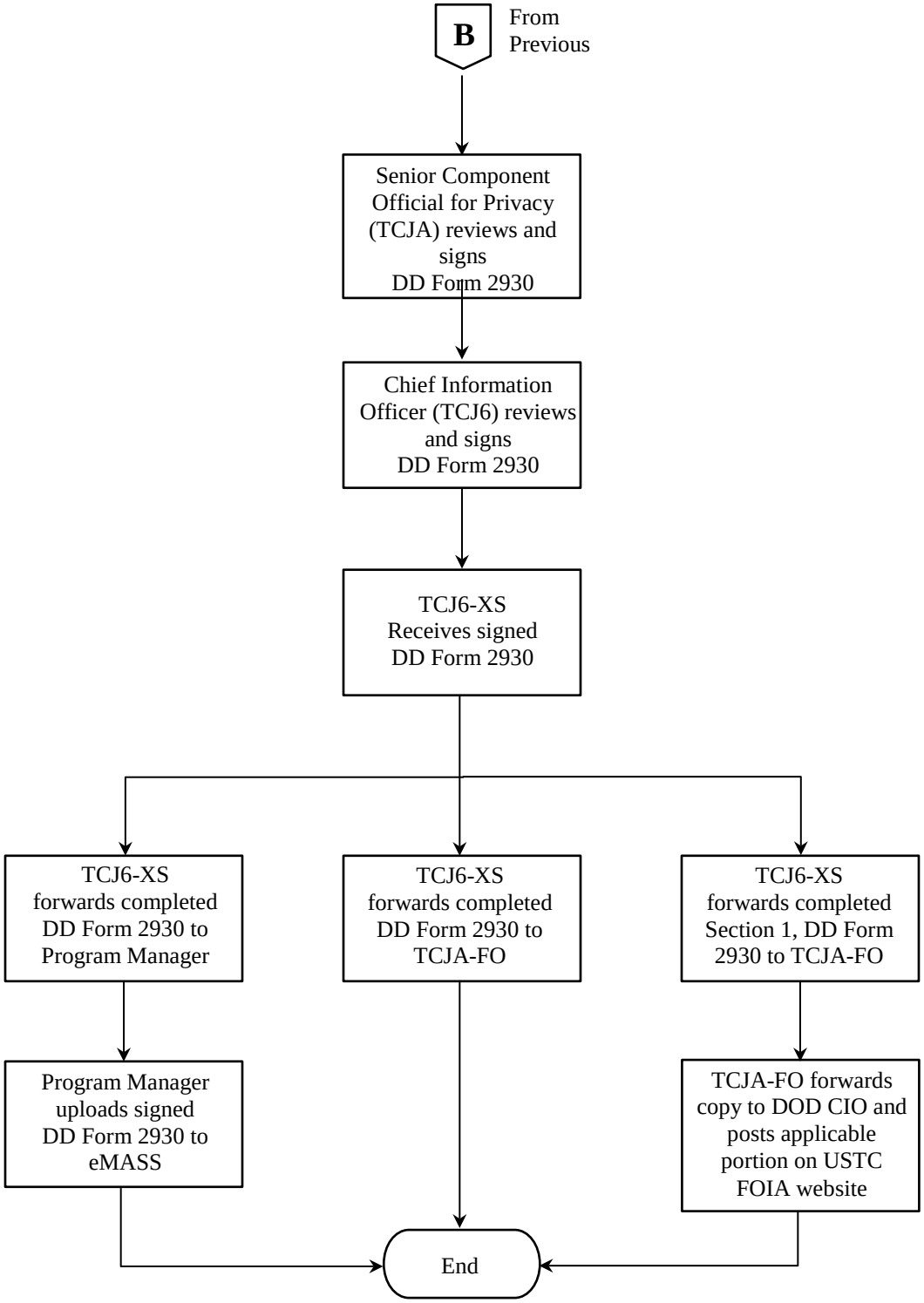
Privacy Impact Assessment (PIA). Is an analysis of how information is handled: to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing or disposing of 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). 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.).

Attachment 2

DD FORM 2930 SUBMISSION AND STAFFING PROCESS – PIA REQUIRED




B
From Previous
Senior Component Official for Privacy (TCJA) reviews and signs DD Form 2930
Chief Information Officer (TCJ6) reviews and signs DD Form 2930
TCJ6-XS Receives signed DD Form 2930
TCJ6-XS forwards completed DD Form 2930 to Program Manager
TCJ6-XS forwards completed DD Form 2930 to TCJA-FO
TCJ6-XS forwards completed Section 1, DD Form 2930 to TCJA-FO
Program Manager uploads signed DD Form 2930 to eMASS
TCJA-FO forwards copy to DOD CIO and posts applicable portion on USTC FOIA website
End

Attachment 3

DD FORM 2930 SUBMISSION AND STAFFING PROCESS – PIA NOT REQUIRED