



## Defense Threat Reduction Agency

8725 John J. Kingman Road, MSC 6201  
Fort Belvoir, VA 22060-6201

DTRA 5400.11  
NOV 13 2007  
DIR-COSM-F

### DTRA INSTRUCTION 5400.11

SUBJECT: Defense Threat Reduction Agency (DTRA) Privacy Program

- References:
- (a) DTRA Instruction 5400.11, "Defense Threat Reduction Agency Privacy Program, January 18, 2000 (hereby cancelled)
  - (b) Section 552a of Title 5, United States Code, "The Privacy Act of 1974" as amended
  - (c) Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources"
  - (d) Department of Defense (DoD) Regulation 5400.11-R, "DoD Privacy Program," May 14, 2007
  - (e) Department of Defense (DoD) Directive 5400.11, "DoD Privacy Program," May 8, 2007
  - (f) OSD Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007

#### 1. PURPOSE

This Instruction supersedes reference (a) and implements DTRA policies, responsibilities, and procedures in accordance with references (b) through (f) to provide guidance for use in compliance with the Privacy Program throughout DTRA.

#### 2. APPLICABILITY

2.1. This Instruction applies to all Department of Defense (DoD) military and civilian employees assigned to DTRA and any of its duty locations. Contractors and its employees are considered to be employees of DTRA for purposes of this Instruction during the performance of the contract. Hereinafter, all of the above are referred to collectively as "DTRA personnel."

2.2. This instruction applies to record systems, to include IT systems, maintained by DTRA, and governs the collection, and dissemination of information contained in DTRA record systems, from which information about an individual is retrieved by a personal identifier.

#### 3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 1.

#### 4. POLICY

4.1. Individuals have a personal and fundamental right to privacy that shall be respected and protected. Accordingly, DTRA's need to collect, maintain, use, or disseminate personal information about individuals for purposes of discharging its statutory responsibilities shall be balanced against the right of the individual to be protected from unwarranted invasions of their privacy.

4.2. DTRA personnel will affirmatively protect individual's legal rights when collecting, maintaining, using, or disseminating personal information. DTRA personnel and systems' managers shall further be advised of the established DoD Privacy Program "Rules of Conduct" set out in Enclosure 3 to reference (e). A notice describing each system of records for which DTRA is responsible shall be published in the "Federal Register" as required by Section 552a of Title 5 of the U.S.Code, OMB Circular A-130, and DoD 5400.11-R, Privacy Program Regulation.

4.3. Appropriate administrative, technical, and physical safeguards shall be established, regardless of the media (e.g., paper, electronic, etc.) involved, to ensure the security and confidentiality of the records to prevent compromise or misuse during storage or transfer.

4.4. Both the DTRA Privacy Officer (COSM-F) and the Security and Counterintelligence (SC) Directorate shall be notified immediately should protected personal information be lost, stolen, or compromised. Reports will then be dispatched, in accordance with reference (f) and paragraph C10.6. of reference (d), to the following: United States Computer Emergency Readiness Team (US CERT), Department of Homeland Security, within one hour; Senior Component Privacy Official (COSM) within 24 hours; and Defense Privacy Office (DPO) and DTRA Director within 48 hours. The DTRA Director or, as appropriate, the Associate Director of an Enterprise, Directorate, or DTRA Field Office shall notify the affected individual(s) within ten days of such a breach. Moreover, if the breach involves a government authorized credit card, the issuing bank shall also be notified.

## 5. RESPONSIBILITIES

### 5.1. The Director shall:

5.1.1. Allocate adequate funding and personnel to establish and support an effective Privacy Program.

5.1.2. Appoint a senior official to serve as the Agency Privacy Act Officer.

5.1.3. Notify the affected individual(s) within ten days of a breach of protected personal information.

### 5.2. The Deputy Director shall:

5.2.1. Serve as the Agency Appellate Authority, responsible for reviewing and making the final decision on all Privacy Act (PA) appeals of initial denials.

5.3. The Chief Mission Support, Office of the Chief of Staff shall:

5.3.1. Administer the implementation of the agency's privacy program in accordance with the specific requirements set forth in references (b) through (f) and this instruction.

5.3.2. Ensure procedures are established to implement this instruction and DoD Directive 5400.11 to comply with the requirements of Section 552a of Title 5 U.S.C. and OMB Circular A-130.

5.3.3. Verify that the DTRA Privacy Program is periodically reviewed by the DTRA Inspector General or other appropriate officials, who shall have specialized knowledge of the DoD Privacy Program.

5.3.4. Serve as the Agency initial denial authority.

5.4. The Privacy Act Officer shall:

5.4.1. Establish procedures and manage activities in support of the DTRA Privacy Program in accordance with references (b) through (f) and this Instruction.

5.4.2. Provide operational support, guidance, and assistance to system managers for responding to PA requests for access/amendment of records.

5.4.3. Direct the day-to-day activities of the DTRA Privacy Program.

5.4.4. Prepare and submit proposed new, alternate, and amended PA systems of records notices for submission, through the DPO, for publication in the Federal Register consistent with Section 552a of Title 5 U.S.C., OMB Circular A-130 and DoD 5400.11-R.

5.4.5. Prepare and submit proposed DTRA privacy rule-making to include documentation for submission of the proposed rule, through the DPO, to the office of the Federal Register for publication, consistent with The Privacy Act of 1974.

5.4.6. Provide advice and support to DTRA elements to ensure that:

5.4.6.1. All information requirements developed to collect and/or maintain personally identifiable information conform to DoD Privacy Program standards;

5.4.6.2. Appropriate procedures and safeguards shall be implemented to protect personally identifiable information to be stored in either a manual and/or automated system of records or transferred by electronic or non-electronic means;

5.4.6.3. When notification is deemed necessary, ensure SC Directorate has reported to US CERT, Department of Homeland Security, within one hour, the COSM is advised within 24 hours, the DPO and DTRA Director are notified within 48 hours, and affected individuals are

informed within ten days when protected personal information is lost, stolen, or compromised;  
and

5.4.6.4. Ensure specific procedures and safeguards are followed regarding the collection and maintenance of personally identifiable information for research purposes.

5.4.7. Ensure that reviews are conducted, and that reports are prepared and submitted consistent with the requirements in references (b) through (f), and as otherwise directed by the DPO.

5.4.7.1. Coordinate on all Privacy Impact Assessments (PIA) the Chief Information Officer (CIO) submits for review and final approval. Evaluate the PIA to ensure the proper balance is struck between an individual's personal privacy and DTRA's information requirements.

5.4.7.2. Provide DTRA's input to the DPO on the privacy portion of OMB's Federal Information Security Management Act (FISMA) Report.

5.4.8. Establish PA training programs with on-line availability through the DTRAnet and ensure that all DTRA personnel, specifically those individuals having primary responsibility for DTRA PA Records Systems, are made aware of the training, as required by references (b) through (f).

5.4.9. Serve as the principal point of contact in the coordination of privacy and related matters.

5.5. The Associate Directors, Special and Staff Office Chiefs shall:

5.5.1. Support the DTRA Privacy Program to ensure all DTRA personnel complete PA training and are made aware of the rules of conduct provided in Enclosure 2.

5.5.2. Appoint an appropriate individual to serve as PA Point of Contact within their purview.

5.5.3. Initiate prompt, constructive management actions on agreed-upon actions identified in agency PA Reports.

5.5.4. When protected personal information is lost, stolen, or compromised and the DTRA Director so designates, notify the affected individual(s) within ten days of the breach.

5.6. The Office of the Chief Information Officer shall:

5.6.1. Ensure that all personnel who have access to information from an automated system of records, during processing, or who are engaged in developing procedures for processing such information, are aware of the provisions of this instruction and are adequately trained on PA requirements.

5.6.2. Coordinate all privacy issues with the Privacy Officer and promptly notify automated system managers and the PA Officer whenever there are changes to agency information technology that may require the submission of an amended system notice for any PA system of records.

5.6.3. Ensure compliance with the rules of conduct for Agency personnel involved in the design, development, operation, or maintenance of any automated system of records and train them in these rules of conduct.

5.6.4. Provide guidance to DTRA officials on the conduct of PIAs and oversee DTRA PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of information in identifiable form in that system, and the risk of harm for unauthorized release of that information. Also, the DTRA CIO reserves the right to request that a PIA be completed on any system that may contain personally identifiable information.

5.7. Agency PA System Managers and DTRA personnel shall exercise the Rules of Conduct as specified in Enclosure 2.

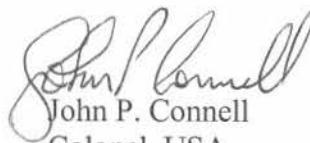
6. PROCEDURES

Procedures and sanctions are set forth in references (b) through (f).

7. EFFECTIVE DATE:

This instruction is effective immediately.

FOR THE DIRECTOR:

  
John P. Connell  
Colonel, USA  
Chief Of Staff

Enclosures – 2

E1. Definitions

E2. Rules of conduct

E1. ENCLOSURE 1DEFINITIONS

E1.1. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Corporations, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals".

E1.2. Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., 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, biometric records, including any other personal information which is linked or linkable to a specified individual).

E1.3. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by DTRA, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particulars assigned to the individual, such as finger or voice print or a photograph.

E1.4. System Manager. The DTRA official who is responsible for the operation and management of a system of records.

E1.5. System of Records. A group of records under the control of DTRA from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual. System notices for all Privacy Act systems of records must be published in the Federal Register.

E1.6. Lost, Stolen, or Compromised Information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for another than authorized purpose where one or more individuals will be adversely affected. Such incidents also are known as breaches.



E2. ENCLOSURE 2

RULES OF CONDUCT

E2.1. DTRA Personnel shall:

E2.1.1. Take such actions, as considered appropriate, to ensure that personal information contained in a system of records, to which they have access or are using incident to the conduct of official business, shall be protected, so that the security and confidentiality of the information shall be preserved.

E2.1.2. Not disclose any personal information contained in any system of records except as authorized by DoD 5400.11-R, Privacy Program, or other applicable law or regulation. Personnel willfully making such a disclosure when knowing the disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

E2.1.3. Report any unauthorized disclosure of personal information from a system of records or the maintenance of any system of records that are not authorized by the Instruction to the DTRA PA Officer.

E2.2. DTRA System Managers for each System of Records shall:

E2.2.1. Ensure that all personnel who have access to the system of records or who develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities and are properly trained to safeguard personal information being collected and maintained under the DTRA Privacy Program.

E2.2.2. Promptly notify the PA Officer of any required new, amended, or altered PA system of records system notices to the DPO for submission in the Federal Register.

E2.2.3. Not maintain any official files on individuals, which are retrieved by name or other personal identifier, without first ensuring that a corresponding notice for the PA system of records shall have been published in the Federal Register. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by Section 552a of Title 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)), is subject to possible criminal penalties and/or administrative sanctions.