



DEFENSE INFORMATION SYSTEMS AGENCY
P.O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

DISA INSTRUCTION 210-225-2*

16 February 2007

INFORMATION SERVICES

Privacy Program

1. **Purpose.** This Instruction prescribes policy, assigns responsibilities, and provides procedures for the Privacy Program for DISA. It also includes guidance on individual access to Privacy Act Information.
2. **Applicability.** This Instruction applies to DISA and DISA *contractors*.
3. **Authority.** This Instruction is published in accordance with the authority contained in DoD Directive 5400.11, Department of Defense Privacy Program, *16 November 2004*, and DoD 5400.11-R, Department of Defense Privacy Program, 31 August 1983.
4. **Definitions.** Definitions are provided in [enclosure 1](#).
5. **Policy.** To comply with 5 U.S.C. 552a, Privacy Act of 1974, DISA will:
 - 5.1 Preserve the personal privacy of individuals and maintain in its records only information about an individual which is relevant and necessary to comply with a Federal statute, Executive Order (E.O.) of the President, or implementing Directives, Regulations, and Instructions. Ensure the information is relevant, timely, complete, and accurate for its intended use.
 - 5.2 Collect information about an individual, to the greatest extent practicable, directly from the individual, when the information may result in adverse determinations about the individual's rights, benefits, or privileges. Inform the individual why the information is being collected, the authority for the collection, what uses will be made of the information, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

5.3 Ensure no records are maintained that describe how individuals exercise rights guaranteed by the First Amendment to the Constitution of the United States, unless expressly authorized by statute, or by the individual about whom the record is maintained, and unless pertinent to, and within the scope of, an authorized law enforcement activity.

5.4 Ensure records contained in a system of record are not disclosed to anyone other than to those who require the records for official purposes, in conformance with the routine uses for such records as published in the Federal Register.

5.5 Except as identified in [paragraph 7](#), permit individuals to know what records pertaining to them exist within DISA and to have access to and have a copy made of all or any portions of such records, to correct or amend such records, and to appeal a denial of access or a request for amendment. (Guidance on individual access to Privacy Act information is provided in [enclosure 2](#).)

5.6 Protect from disclosure any personal information contained in any system of records except as authorized by this Instruction. (The DoD Blanket Routine Uses at 32 CFR part 310, Appendix C to DoD 5400.11-R [authority document], applies to all DISA systems of records unless specifically excluded in the records notice.)

5.7 Ensure a notice for the system of records has been published in the Federal Register before maintaining files and listings that contain information about individuals and are retrievable by name or other personal identifier.

5.8 Report to the appropriate Privacy Act official any disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this Instruction.

5.9 Ensure computer matching programs and Privacy Protection Act data shared among the Federal Government agencies will benefit one of the agencies by disclosing an individual has received benefits in excess of those they may be entitled to obtain as requirements of section 552a of 5 U.S.C., Privacy Act of 1974, as amended; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Requirements; and DoD 5400.11-R (authority document).

6. Privacy Standards of Conduct. The following standards of conduct are to be observed whenever using or having access to information of a personal nature or pertaining to a particular individual or individuals.

6.1 Personal information about any individual, whether in a system of records or not, is to be safeguarded and protected so that the security and confidentiality of the information is preserved and its use limited to official uses.

6.2 Disclosure of personal information contained in any system of records is to be prevented, except as authorized by section 32 CFR part 310 (DoD 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.

6.3 Disclosure of personal information from a system of records or the maintenance of any system of records that is not authorized by this Instruction is to be reported to the appropriate DISA Privacy Act Officer.

7. Exemptions Applying to Certain Privacy Act Records.

7.1 Individual access to record contents is to be denied in the circumstances described below:

7.1.1 Properly classified national security information shall be exempt from disclosure under section (k)(1) of 5 U.S.C. 552a to the extent that the system contains any information properly classified under E.O. 12958 and that is required by that E.O. to be kept classified in the interest of national defense or foreign policy. (This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein, which contain isolated items of properly classified information.)

7.1.2 Information compiled or maintained in reasonable anticipation of civil or criminal actions or proceedings or otherwise shall be exempt under 5 U.S.C. 552a(d)(5). (Requests for pending investigations will be denied and the requester instructed to forward another request giving adequate time for the investigation to be completed.)

7.1.3 In addition to the exemptions stated in subparagraphs 7.1.1 and 7.1.2, the following types of information shall be exempt from disclosure: that which would compromise the

identity of confidential sources; that which would alert subjects of an investigation of an actual or potential criminal or civil violation to the investigation; that which would endanger the physical safety of witnesses, informants, and law enforcement personnel; that which would violate the privacy of third parties; and that which would otherwise impede effective law enforcement.

7.2 Information exempt from disclosure will be deleted from the requested documents and the balance made available, whenever possible.

8. Remedies That May Be Invoked by an Individual Claiming Violation of Privacy Act Rights. The following are provisions of the Privacy Act that may be invoked to effect relief when an individual claims the Agency or its employees have violated his or her privacy rights.

8.1 Administrative. An individual is permitted to seek relief through appropriate administrative channels.

8.2 Civil Actions and Remedies. An individual may file a civil suit (see 5 U.S.C. 552a(g)). (In addition to specific remedial actions, the Privacy Act provides for the payment of damages, court cost, and attorney fees in some cases.)

9. Criminal Penalties. The Privacy Act also provides for criminal penalties. (See 5 U.S.C. 552a(1).)

9.1 Any employee who by virtue of his or her employment or official position, has possession of, or access to, agency system of records which contain individually identifiable information, knowing that dissemination is prohibited, to anyone not entitled to receive the information, maybe guilty of a misdemeanor and fined not more than \$5,000.

9.2 Any employee who willfully maintains a system of records without publishing the required systems notice in the Federal Register will be guilty of a misdemeanor and fined not more than \$5,000.

9.3 Any individual who knowingly and willfully requests or obtains any record concerning an another individual under false pretenses maybe found guilty of a misdemeanor and fined not more than \$5,000.

10. Responsibilities.

10.1 **Chief Information Officer (CIO)/Director for Strategic Planning and Information (SPI).** The CIO/Director, SPI, will:

10.1.1 Direct and administer the DISA Privacy Program.

10.1.2 Serve as the DISA principal point of contact for administrative Privacy Act matters.

10.1.3 Ensure an internal DISA Privacy Program is maintained and all echelons of DISA effectively comply with this Instruction.

10.1.4 Publish, as necessary, internal Privacy Act procedures that are consistent with DoDD 5400.11 and DoD 5400.11-R (authority documents).

10.1.5 Provide policy guidance to Systems Managers for processing internal Privacy Act requests.

10.1.6 Prepare Privacy Act reports for DoD and other authorities, as required.

10.1.7 Prepare required Privacy Act system notices and amendments for submission to the Federal Register. ([Subparagraph 12.1](#) provides additional details.)

10.1.8 Assign a skilled individual as Privacy Officer to carry out the administrative management responsibility of the privacy program on behalf of the CIO.

10.2 **Chief of Staff (COS).** The COS, as the Privacy Act Appeal Authority, will dictate internal appeal procedures.

10.3 **General Counsel (GC).** The GC will:

10.3.1 Serve as the DISA principal point of contact for legal and litigations matters related to the Privacy Act.

10.3.2 Be the final authority within DISA on all legal opinions regarding the Privacy Act or its implementation.

10.3.3 Render legal opinions to the CIO, the Privacy Act Appeal Authority, and other DISA elements, as appropriate.

10.3.4 Represent DISA on the Defense Privacy Board.

10.3.5 Review all Privacy Act denials of requests to ensure uniformity and consistency in legal positions and interpretations rendered.

10.3.6 Review all Privacy Act notices and amendments prior to submission to the Defense Privacy Office for publication in the Federal Register.

10.3.7 Approve all Privacy Act statements prior to their reproduction and distribution.

10.4 Principal Directors of Strategic Business Units, Directors and Chief of Shared Services Units, Directors of Program Executive Offices, Direct Reports, and Special Advisors, Headquarters, DISA; Commanders and Director of Special Missions; and Commanders of DISA Combatant Command Field Offices. These individuals will:

10.4.1 Designate a Privacy Officer Coordinator to be responsible for Privacy Act matters in their organizations. (The name of the Privacy Officer Coordinator should be provided to the CIO.)

10.4.2 Ensure their directorate Privacy Officer Coordinator and System Managers acquire the necessary training to administer the Privacy Act.

10.4.3 Receive, process, and respond, as appropriate, to Privacy Act requests from employees and from CIO within 10 working days.

10.4.4 Coordinate with CIO on any newly proposed record systems or on changes to existing systems.

10.4.5 Collect and forward to CIO the information necessary to prepare reports, when requested.

10.4.6 Respond promptly to decisions on granting access to records, amending records, or filing statements of disagreement.

11. Duties.

11.1 System Manager. A System Manager will:

11.1.1 Establish and maintain records that can be retrieved by a name or other personal identifier that are contained in a Privacy Act systems of records notice.

11.1.2 Establish appropriate administrative, technical, and physical safeguards to ensure the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected.

11.1.3 Ensure all personnel who handle records containing personal information are Privacy Act trained and know the proper procedures for protecting and safeguarding personal information.

11.1.4 Process Privacy Act requests forwarded by the Privacy Officer.

11.1.5 Maintain a disclosure accounting record for each Privacy Act system of records. ([Subparagraph 12.2](#) provides additional details.)

11.1.6 Provide a copy of any updated system information, including changes to an automated information system, to the Privacy Officer for each system of records.

11.1.7 Ensure all personnel who have access to information from a system of records or who are engaged in developing procedures for processing such information are aware of the provisions of the DoD Privacy Program policies and procedures.

11.1.8 Promptly notify the Privacy Officer of any required new, amended, or altered system notices whenever one is aware of a new requirement for using personal information or an existing requirement or method of files storage changes.

11.1.9 Notify the Privacy Officer, who will in turn notify Defense Privacy Office, when a complaint citing the Privacy Act is filed in a U.S. District Court against DISA. ([Subparagraph 12.3](#) provides additional details.)

11.1.10 Notify an individual as soon as possible, but no later than 10 working days, after the loss, theft, or compromise of protected personal information is discovered and advise the individual as to what specific data was involved, the circumstances surrounding the loss, theft, or compromise, and what protected actions the individual can take.

11.2 Privacy Officer and Privacy Officer Coordinator.

11.2.1 **Privacy Officer.** The Privacy Officer reports to the SPI Chief, Strategy and Policy Division (SPI3), and will:

11.2.1.1 Maintain liaison with the DoD Privacy Office.

11.2.1.2 Serve as the local point of contact on administrative matters relating to the Privacy Act.

11.2.2 Privacy Coordinator (PC) and Alternate Privacy Coordinator (APC). These individuals will:

11.2.2.1 Maintain an inventory of the internal system of records for their organization that contains privacy information.

11.2.2.2 Work closely with the Privacy Officer to ensure their organization receives annual privacy act training.

11.2.2.3 Conduct internal organizational reviews to ensure privacy information is properly managed and protected.

12. Recordkeeping and Reporting. The following records and reports are required to comply with provisions of the Privacy Act and implementing regulations.

12.1 Privacy Act System Notice. A Privacy Act system notice must be published in the Federal Register whenever a system of records is implemented or changed. This includes changing from a manual to an automated system. (The format for the system notice is contained in Appendix 5 of DoD 5400.11-R [authority document].)

12.2 Disclosure Accounting Record. The disclosure accounting record contains the following information pertaining to release of the personal information in the file: dates the record was disclosed; description of the information released; purpose of the disclosure; and name and address of the person or agency to whom the disclosure was made. The disclosure accounting record is maintained for 5 years or the life of the record disclosed, whichever is longer. (An individual requesting a record may also request the associated disclosure accounting record and is entitled to receive this record unless a published exemption to the Privacy Act system notice would prohibit such release.)

12.3 Litigation Status Sheet. A litigation status sheet is used by the System Manager to keep the Privacy Officer apprised of legal developments concerning complaints lodged against the Agency under the Privacy Act. (The format is found in Appendix 8 of DoD 5400.11-R [authority document].) A revised litigation status sheet is provided at each stage of the litigation. When a court renders a formal opinion or judgment,

copies of the opinion or judgment are to be provided to the Defense Privacy Office via the Privacy Program Office and office of the General Counsel with the latest litigation status sheet, which includes the report of that opinion or judgment.

13. Submission of a Privacy Act Request.

13.1 Internal Privacy Act Request.

13.1.1 A request to obtain records from a system of records or to inspect a list of previous disclosures of records will be in writing. The request will normally be submitted directly to the System Manager in the office holding the record.

13.1.2 An individual's written request for access to or copies of records about himself or herself that does not specify the Privacy Act or the Freedom of Information Act (FOIA) under which the request is made will be processed as a Privacy Act request.

13.2 External Privacy Act Request.

13.2.1 A request for access to records in a system of records will be in writing and will be directed to the CIO. In the case of a request received by mail, a notarized statement or unsworn declaration in accordance with 28 U.S.C. 1746 proving the personal identity of the requester may be required.

13.2.2 A request from contractor personnel seeking explanation as to why they were not cleared for access and which does not mention either the Privacy Act or the FOIA will be referred to the Personnel, Manpower, and Security Directorate (MPS) Security Manpower Division (MPS6) for reply.

13.2.3 A request from nonhired applicants seeking an explanation as to why they were not hired and which does not mention either the Privacy Act or the FOIA will be referred to the MPS Civilian Personnel Division (MPS1) for reply.

14. Appeal of Denial of Access to Privacy Act Information.

14.1 Any individual denied access to requested records may appeal the initial decision to the Privacy Act Appeal Authority within 60 calendar days of the date of the denial of access notification. A written determination will be issued to the appellant within 30 working days of the date of appeal or when all necessary information has been provided by the requester.

14.2 If the Appeal Authority cannot make a fair and equitable review within 30 days, the appellant will be notified in writing of the decision to extend the period of review, the reasons for the delay, and when the appellant may expect an answer. If the appeal is granted, the appellant will be notified in writing and granted access to the denied material.

14.3 If the Appeal Authority decides that the request for access should be denied, the recommendation of the Appeal Authority will be forwarded to the Vice Director.

14.4 The Vice Director makes a final determination which will be provided to the requester through the office of the General Counsel (GC). The office of the GC will ensure the notification complies with the appeals provisions contained in DoD 5400.11-R (authority document).

15. Amendment of Records in a Privacy Act System of Records. Minor factual errors in an individual's personal records may be corrected routinely upon request without resort to the Privacy Act or to the provisions of this Instruction, provided the requester and the record holder agree to the procedure and the requester receives a copy of the corrected record whenever possible. Requests for deletions, removal of records, and amendment of substantive factual information will be processed in accordance with the provisions below.

15.1 A request submitted under the Privacy Act for amendment of a record containing substantial factual error, because the information is incorrect or incomplete, will be in writing and will be acknowledged within 10 working days of receipt of the request by the System Manager of the record containing the information to be amended. The request should be reviewed and the requester advised of the result of the review within 10 working days. If additional time is needed (normally no more than 30 working days), the requester will be so advised.

15.2 If the System Manager agrees with the request, he or she notifies the requester and promptly amends the record and notifies all holders and recipients of the records that the correction was made. The amendment procedure is not intended to replace other procedures such as those for registering grievances or appealing performance appraisal ratings.

15.3 If the System Manager refuses to amend any part of a record, he or she promptly notifies the requester of the refusal and states the reason(s). The System Manager informs the requester of the procedures for requesting a review of the decision by the Privacy Act Appeal Authority.

15.4 Upon receipt of an appeal of a denial to amend a record, the Privacy Act Appeal Authority renders a decision within 30 working days except when circumstances require an extension. If an extension is necessary, the requester will be informed in writing of the reasons for the delay and of the appropriate date on which the review is expected to be completed.

15.5 If the Privacy Act Appeal Authority denies the request for amendment, in whole or in part, that person promptly forwards the recommendation to the Vice Director.

15.6 The Vice Director makes a final determination and, through the office of the GC, notifies the requester in writing of the decision. The Office of the GC ensures the notification complies with the appeals procedure contained in DoD 5400.11-R (authority document).

16. Privacy Act Training Requirements. To meet Privacy Act training requirements for individuals having differing functions in DISA, three levels of Privacy Act training will be provided as follows:

16.1 Orientation. Training that provides basic understanding of this Instruction as it applies to the individual's job performance. This training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

16.2 Specialized. Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to, personnel specialists, finance officers, DISA personnel who may be expected to deal with the news media or the public, special investigators, paperwork managers, and other specialists (reports, forms, records, and related functions), computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, and anyone responsible for implementing or carrying out special functions. Specialized training should be provided on a periodic basis.

16.3 **Management.** Training designed to identify for managers (such as, senior system managers) considerations that they should take into account when making management decisions regarding the DISA Privacy Program.

FOR THE DIRECTOR:

2 Enclosures a/s


MARK S. BOWMAN
Brigadier General, USA
Chief of Staff

Change List:

Paragraph 2 - DISA contractors now included.

Paragraph 9 - Reflects DoD Privacy Act polices.

Enclosure 1 - Definitions added.

*This Instruction cancels DISAI 210-225-2, 22 October 2003.

OPR: SPI

DISTRIBUTION: Y

Return to:

[Top of DISAI 210-225-2 Basic](#)

[DISAI 210-225-2 Enclosure 1](#)

[DISAI 210-225-2 Enclosure 2](#)

[Publications Listing](#)

[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 18 February 2007

DEFINITIONS

Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

Agency. For the purpose of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. However, for all other purposes involving the Privacy Act, the DoD Components are considered independent Agencies. The other purposes include requests by individuals for access and amendment to records pertaining to them, denial of access or amendment to such records, appeals from denials, and the recordkeeping documenting access actions by system managers and Privacy Act Officials employed by each DoD independent agency.

Computer Match Program. *The computerized comparison of two or more automated systems of records or a system of records with non-Federal records. Manual comparison of systems of records or a system of records with non-Federal records are not covered.*

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 be held in confidence or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

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

Individual. A living 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, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

Individual Access. *Access to information pertaining to the individual by the individual or his or her designated agent of legal guardian.*

Law Enforcement Activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

Lost, Stolen, or Compromised Information. *Actual or possible unauthorized disclosure or personal information either to known or unknown persons whether or not a potential exists that the information may be used for unlawful purposes to the detriment of the individual.*

Maintain. In the context of the Privacy Act, "maintain" includes collecting, using, or disseminating, as well as just keeping and holding, personal information contained in a Privacy Act system of records.

Official Use. Within the context of this Instruction, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R, DoD Information Security Program Regulation.

Personal Information. Information about an individual that identifies, 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, personnel, medical, and financial information; etc.

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.

Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, 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 particular assigned to the individual, such as a finger or voice print or a photograph.

Risk Assessment. *An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.*

Routine Use. The disclosure of a record outside DoD for a use that is compatible with the purpose for which the information was collected and maintained by DoD. The routine use must be included in the published system notice for the system of records involved.

System Manager. The DoD component official who is responsible for the operation and management of a system of records.

System of Records. A group of records under the control of a DoD component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

Return to:

[Top of DISAI 210-225-2 Enclosure 1](#)

[DISAI 210-225-2 Basic](#)

[DISAI 210-225-2 Enclosure 2](#)

[Publications Listing](#)

[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 18 February 2007

INDIVIDIAL ACCESS TO PRIVACY ACT INFORMATION

1. If an individual has been given access to his or her personnel file as a result of a Privacy Act request, the file will continue to be available to the individual for review without the submission of a second request.
2. A requester does not need to state a reason or otherwise justify a Privacy Act request and may be accompanied by another person when Privacy Act records are requested in person rather than in writing. In this case, the requester may be required to furnish a statement authorizing discussion of the records in the presence of the other person. If a requester asks another person to obtain a record on his or her behalf, the requester must provide a notarized statement appointing that person as his or her representative, authorizing the person access to the record, and affirming that such access will not constitute an invasion of the requester's privacy or a violation of rights under the Privacy Act.
3. The requester will not be charged a fee for making a readable copy to satisfy the request, to review a record, or to provide a copy in response to a request by mail.
4. A medical record will be disclosed to the individual to whom it pertains unless the System Manager determines providing the record could have an adverse effect on the requester. In such case, the requester will be advised the information will be sent to a doctor named by the requester. If the doctor refuses to disclose the record to the patient, the requester must provide a statement to the System Manager noting the doctor's refusal. At this point, the System Manager must provide the requested record directly to the requester.
5. An individual requesting access to investigatory records compiled by another agency, but in the custody of DISA, will be referred to the originating agency.
6. An individual is not entitled to have access to any information compiled in reasonable anticipation of a civil action or proceeding nor is an individual entitled to have a record created in response to a request for information.

7. Requesting or obtaining access to records under false pretenses is a violation of the Privacy Act and is subject to criminal penalty.

8. Copies of classified records will be released only to persons authorized to receive such material.

Return to:

[Top of DISAI 210-225-2 Enclosure 2](#)

[DISAI 210-225-2 Basic](#)

[DISAI 210-225-2 Enclosure 1](#)

[Publications Listing](#)

[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 18 February 2007
