INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

January 29, 2010

INSPECTOR GENERAL INSTRUCTION 5400.11

PRIVACY ACT PROGRAM

FOREWORD

This Instruction provides guidance and procedures for implementing the Privacy Program within the Department of Defense Office of Inspector General.

The office of primary responsibility for this Instruction is the Office of Communications and Congressional Liaison. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Stephen D. Wilson
Assistant Inspector General
for Administration and Management

PRIVACY ACT PROGRAM

TABLE OF CONTENTS

Paragraph **Page**

CHAPTER 1. GENERAL

CHAPTER 2. PROCEDURES

APPENDICES

CHAPTER 1
GENERAL

A. Purpose. This Instruction provides the Department of Defense Office of Inspector General (DoD OIG) with guidance and procedures for implementing the Privacy Act Program, in accordance with (IAW) the authority in reference (a), and to implement the policies and procedures outlined in references (b) and (c).

B. References. See Appendix A.

C. Definitions. See Appendix B.

D. Acronyms. See Appendix C.

E. Cancellation. This Instruction supersedes IGDINST 5400.11, *Privacy Act Program*, May 11, 2006.

F. Applicability. This Instruction applies to the Office of Inspector General and the Department of Defense Inspector General Components, hereafter referred to collectively as the OIG Components. It covers systems of records maintained by the Components and governs the maintenance, access, change, and release of information contained in those systems of records, from which information about an individual is retrieved by a personal identifier.

G. Policy. It is OIG policy that:

1. Personal information contained in any system of records maintained by any Component shall be safeguarded. An individual shall be permitted to the extent authorized by references (c) and (d):

   a. Determine what records pertaining to them are contained in a system of records.

   b. Gain access to such records and obtain a copy of those records or a part thereof.

   c. Correct or amend such records that are not relevant, accurate, timely, or complete and obtain a copy of those records or a part thereof.

   d. Appeal a denial of access or a request for amendment.

2. Each office maintaining records and information about individuals shall ensure that this data is protected from unauthorized disclosure of personal information. These offices shall permit individuals to have access to and have a copy made of all or any portion of records about them, except as provided in Chapters 3 and 5 of reference (c). The individuals shall also have an opportunity to request that such records be amended.

3. Necessary records of a personal nature that are individually identifiable, shall be maintained in a manner that complies with the law and OIG policy. Any information collected by the Components shall be as accurate, relevant, timely, and complete as is reasonable to ensure fairness to the individual. Adequate safeguards shall be provided to prevent misuse or unauthorized release of such information.

4. The Privacy Office, within the Freedom of Information Division (FOID), shall be responsible for implementing the OIG Privacy Program.

H. Responsibilities

1. The **Assistant Inspector General (AIG), Office of Communications and Congressional Liaison (OCCL)** shall:

a. Serve as the appellate authority for the Components when a requester appeals a denial for access, as well as, when a requester appeals a denial for amendment or initiates legal action to correct a record.

b. Coordinate with the Office of General Counsel (OGC) on all proposed appeal decisions.

2. The **Component Heads** shall:

a. Designate an individual in writing as the point of contact for Privacy Act matters and designate an official in writing to deny initial requests for access to an individual's records or changes to records. Advise the Privacy Office of names of officials so designated.

b. Provide opportunities for appointed personnel to attend periodic Privacy Act training.

c. Report any new record system, or changes to an existing system, to the Privacy Office, at least 90 days before the intended use of the system.

d. Formally review each systems of records notice on a biennial basis and update as necessary.

e. Include appropriate Federal Acquisition Regulation and Defense Federal Acquisition Regulation clauses in all contracts that provide for contractor personnel to access the Component records systems covered by the Privacy Act. Such clauses shall provide that such access is subject to the provisions of the Privacy Act and such systems shall be used and maintained in a manner consistent with the Privacy Act.

f. Review all implementing guidance prepared by the Components as well as all forms or other methods used to collect information about individuals to ensure compliance with reference (c).

g. Establish administrative processes in their Component to comply with the procedures listed in this Instruction.

h. Coordinate with the OGC on all proposed denials of access to records.

i. Provide justification to the Privacy Office, when access to a record is denied in whole or in part.

j. Provide the record to the Privacy Office, when the initial denial of a request for access to such record has been appealed by the requester or at the time of initial denial, if an appeal seems likely.

k. Maintain an accurate administrative record documenting the actions resulting in a denial for access to a record or for the correction of a record. The administrative record shall be maintained so it can be relied upon and submitted as a complete record of proceedings if litigation occurs.

l. Provide appropriate Privacy Act training for all personnel when required.

m. Forward all requests for access to records received directly from an individual to the Privacy Office, for processing.

n. Maintain a record of each disclosure of information (except disclosures to DoD personnel for use in the performance of their official duties or under reference (g)) from a system of records.

3. The **Chief, FOID**, shall:

a. Direct and administer the DoD Privacy Program for the Components.

b. Establish standards and procedures to ensure implementation of and compliance with references (b) and (c).

c. Coordinate with the OGC on all Component denials of appeals for amending records and review actions to confirm denial of access to records.

d. Provide advice and assistance to the Components on matters pertaining to reference (d).

e. Direct the Privacy Office to implement all aspects of reference (b) and (c).

4. The **Privacy Office** shall:

a. Exercise oversight and administrative control of the Privacy Act Program for the Components.

b. Provide guidance and training to the Components.

c. Collect and consolidate data from the Components and submit reports to the Defense Privacy Office (DPO).

d. Coordinate and consolidate information for reporting all record systems, as well as changes to approved systems to the DPO for final processing to the Office of Management and Budget, (reference (e)), the Congress, and the Federal Register.

e. Refer all matters about amendments of records and general and specific exemptions to the proper Components.

5. The **Requester** shall:

a. Submit the request in writing. A requester seeking access to records pertaining to him/her, which are filed by name or other personal identifier, may make such a request in writing to the Privacy Office**,** or in person to the custodian of the records. If the requester is not satisfied with the response, he/she may file a written appeal. The requester shall provide proof of identity by showing a driver's license or similar credentials.

b. Describe the record sought and provide sufficient information to enable the material to be located (e.g., identification of system of records, approximate date it was initiated, originating organization, and type of document).

c. Submit a written request to amend a record to the office designated in the system of records notice.

CHAPTER 2
PROCEDURES

A. Publication of Notice in the Federal Register

1. A notice shall be published in the Federal Register of any record system meeting the definition of a system of records.

2. The Component Heads shall submit notices for new or revised systems of records to the Privacy Office, for review at least 90 days prior to desired implementation.

3. The Privacy Office shall forward completed notices to the DPO for review and publication in the Federal Register. Publication in the Federal Register starts a 30 day comment window that provides the public with an opportunity to submit written data, views, or arguments to the Components for consideration before a system of record is established or modified.

B. Access to Systems of Records Information

1. Records shall be disclosed only to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted. If an individual is accompanied by a third party, the individual shall be required to furnish a signed access authorization granting the third party access conditions.

2. Individuals may request access to their records in person or by mail IAW the following procedures:

a. Any individual making a request for access to records in person shall provide personal identification to the appropriate system owner, as identified in the System of Records Notice published in the Federal Register, to verify the individual's identity.

b. Any individual submitting a request by mail for access to information shall address such request to the Department of Defense Office of Inspector General, Privacy Office, 400 Army Navy Drive, Suite 1021, Arlington, VA 22202-4704. To verify the identity of the individual, the request shall include either a signed notarized statement or an unsworn declaration that the requester is the person to whom the requested records pertain.

3. There is no requirement that an individual be given access to records that are not in a group of records that meet the definition of a system of records.

4. Granting access to a record containing personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access.

5. No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

6. Individuals shall not be denied access to a record in a system of records about themselves because those records are exempted from disclosure under reference (f). Individuals may only be denied access to a record in a system of records about themselves when those records are exempted from the access provisions of Chapter 5 of reference (b) .

7. Individuals shall not be denied access to their records for refusing to disclose their Social Security Number (SSN), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, and the SSN was required under a statute or regulation adopted prior to this date for purposes of verifying the identity of an individual, this restriction does not apply.

C. Access to Records or Information in Exempt Systems

1. Requests are processed to give requesters a greater degree of access to records on themselves.

2. Records (including those in the custody of law enforcement activities) that have been incorporated into a system of records, exempted from access, shall be processed IAW paragraph C1.5.13, of reference (f). When access is denied due to a claimed exemption, the request shall be processed to provide information that is releasable under the Freedom of Information Act.

3. Records from systems exempted from access shall be processed under Chapter 5 of reference (c) or reference (f), depending upon which regulation gives the greater degree of access. (See Chapter 3 of reference (c)).

4. Exempt records temporarily in the custody of another Component are considered the property of the originating Component. Access to these records is controlled by the system notices and rules of the originating Component.

D. Access to Illegible, Incomplete, or Partially Exempt Records

1. An individual shall not be denied access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (e.g., deteriorated state or on magnetic tape). The document shall be prepared as an extract, or it shall be exactly recopied.

2. If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

3. When the physical condition of the record makes it necessary to prepare an extract for release, ensure that the extract can be understood by the requester.

4. The requester shall be informed of all deletions or changes to records.

E. Amending and Disputing Personal Information in Systems of Records

1. The Component Head, or an individual specifically designated by the Component Head, i.e, a designated official, shall allow individuals to request amendment to their records to the extent that such records are not accurate, relevant, timely, or complete, unless the system of records has been exempted from the amendment procedures under paragraph C5.1.2. of reference (c). Requests should be as brief and as simple as possible and should contain, as a minimum, identifying information to locate the record, a description of the items to be amended, and the reason for the change. A request shall not be rejected nor required to be resubmitted unless additional information is essential to process the request. Requesters shall be required to provide verification of their identity to ensure that they are seeking to amend records about themselves and not, inadvertently or intentionally, the records of others.

2. The appropriate system manager shall mail a written acknowledgment to an individual's request to amend a record within 10 workdays after receipt. Such acknowledgment shall identify the request and may, if necessary, request any additional information needed to make a determination. No acknowledgment is necessary if the request can be reviewed, processed, and if the individual can be notified of compliance or denial within the 10 day period. Whenever practical, the decision on the request shall be made within 30 workdays. For requests presented in person, written acknowledgment may be provided at the time the request is presented.

3. The Component Head or designated official shall promptly take one of three actions on requests to amend the records:

a. If the Component Head or designated official agrees with any portion or all of an individual's request, he/she shall proceed to amend the records IAW existing statutes, regulations, or administrative procedures and inform the requester of the action taken. The Component Head or designated official shall also notify all previous holders known to be retaining the record or information, that the amendment has been made and shall explain the substance of the correction.

b. If the Component Head or designated official disagrees with all or any portion of a request, the individual shall:

(1) Advise the individual of the denial and the reason for it.

(2) Inform the individual that he/she may appeal the denial.

(3) Describe the procedures for appealing the denial, including the name and address of the official to whom the appeal should be directed to the Department of Defense, Office of Inspector General, Privacy Office, 400 Army Navy Drive, Suite 1021, Arlington, VA 22202-4704. The procedures should be as brief and simple as possible.

(4) Furnish a copy of the justification of any denial to amend a record to the Privacy Office.

c. If the request for an amendment pertains to a record controlled and maintained by another Federal agency, the request shall be referred to the appropriate agency and the requester advised of this.

4. When personal information is disputed by the requestor, the Component Head or designated official shall:

a. Determine whether the requester adequately supported his/her claim that the record is inaccurate, irrelevant, untimely, or incomplete.

b. Limit the review of a record to those items of information that clearly bear on any determination to amend the records and shall ensure all those elements are present before a determination is made.

5. If an individual disagrees with the initial Component determination, he/she may file an appeal. If the record is created and maintained by a Component, the appeal should be sent to the Department of Defense, Office of Inspector General, Privacy Office, 400 Army Navy Drive, Suite 1021, Arlington, VA 22202-4704.

6. If the Privacy Office determines the system of records should not be amended as requested, the Privacy Office shall provide a copy of any statement of disagreement to the extent that disclosure accounting is maintained and shall advise the individual of the following:

a. The reason and authority for the denial.

b. His/her right to file a statement of the reason for disagreeing with the Privacy Office's decision.

c. The procedures for filing a statement of disagreement.

d. The statement filed shall be made available to anyone the record is disclosed to, together with a brief statement of the Component summarizing its reasons for refusing to amend the records.

7. If the Privacy Office determines that the record should be amended IAW the individual's request, the Component shall amend the record, advise the individual, and inform previous recipients, known to be retaining the record or information, where a disclosure accounting has been maintained.

8. All appeals should be processed within 30 workdays after receipt by the proper office. If the Privacy Office determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

F. Disclosure of Disputed Information

1. If the Privacy Office determines the record should not be amended and the individual has filed a statement of disagreement, the Component shall annotate the disputed record so it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record. Where disclosure accounting has been made, the Component shall advise previous recipients, known to be retaining the record or information, that the record has been disputed and shall provide a copy of the individual's statement of disagreement.

a. This statement shall be maintained to permit ready retrieval whenever the disputed portion of the record is disclosed.

b. When information that is the subject of a statement of disagreement is subsequently disclosed, the Component's designated official shall note which information is disputed and provide a copy of the individual's statement.

2. The Component shall include a brief summary of its reasons for not making a correction when disclosing disputed information. Such statement shall normally be limited to the reasons given to the individual for not amending the record.

3. Copies of the Component summary shall be treated as part of the individual's record, however, it shall not be subject to the amendment procedures.

G. Penalties

1. Civil Action. An individual may file a civil suit against the Component or its employees if the individual believes his/her rights under the Privacy Act have been violated.

2. Criminal Action. Criminal penalties may be imposed against an employee for certain offenses as follows: willful and knowing disclosure of protected information **to anyone not entitled to receive it**, willful failure to publish a required **public** notice; and knowing and willful request or obtaining access under false pretenses. An employee may be fined up to $5,000 for a violation.

H. Litigation Status Sheet. Whenever a complaint is filed in a U.S. District Court against the DoD, a Component, or any employee, the responsible system manager shall promptly notify the Privacy Office, which shall notify the DPO. The Privacy Office shall consult the OGC on the preparation of the litigation status sheet (Appendix 8 of reference (c)) and any further requirements. As the OGC is the POC for all OIG litigation matters, the OGC shall be promptly notified of any litigation and shall represent the OIG's interests, to include assisting responsible OIG personnel in responding to related matters.

I. Computer Matching Programs. All requests for participation in a matching program (either as a matching agency or a source agency) shall be submitted to the DPO for review and compliance. The Components shall submit these requests through the Privacy Office.

APPENDIX A
REFERENCES

a. DoDD 5106.01, *Inspector General of the Department of Defense*, April 13, 2006

b. DoDD 5400.11, *DoD Privacy Program*, May 8, 2007

c. DoD 5400.11-R, *Department of Defense Privacy Program*, May 14, 2007

d. Title 5, United States Code, section 552a, *The Privacy Act of 1974*

e. Appendix I of Office of Management and Budget Circular No. A-130, *Federal Agency Responsibilities for Maintaining Records about Individuals*, February 8, 1996

f. DoD 5400.7-R, *DoD Freedom of Information Act Program*, September 4, 1998

g. Title 5, United States Code, section 552, *The Freedom of Information Act*

APPENDIX B
DEFINITONS

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

2. **Agency**. For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the DoD is a considered a single agency. For all other purposes, to include requests for access and amendment, denial of access, or amendment, appeals from denials, and record keeping, as relating to the release of records to non-DoD Agencies, each DoD Component is considered an agency.

3. **Computer Matching 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.

4. **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.

5. **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 may also act on behalf of an individual. Members of the U.S. Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals" when acting in an entrepreneurial capacity with the DoD, but are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits, etc.).

6. **Maintain**. The term "maintain" includes maintain, collect, use or disseminate, 5 U.S.C. § 552a(a)(3).

7. **Personal Information**. Information about an individual that identifies, links, relates, or is unique to, or describes him/her (i.e., a SSN; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc). Such information also is known as personally identifiable information (e.g., information that can be used to distinguish or trace an individual's identity, such as his/her name; SSN; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual).

8. **Record**. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his/her education, financial transactions, medical history, and criminal or employment history and that contains his/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, 5 U.S.C. § 552a(a)(4).

9. **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 shall be included in the published system notice for the system of records involved.

10. **Source Agency**. Any agency that discloses records contained in a system of records to be used in a computer-matching program, or any state or local government or agency thereof, which discloses records to be used in a computer matching program.

11. **System Manager**. A Component Head or designated official who has overall responsibility for a system of records. The system manager may serve at any level in the OIG. Systems managers are indicated in the published systems of records notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity).

12. **System of Records**. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, 5 U.S.C. § 552a(a)(5).

APPENDIX C
ACRONYMS

DoD	Department of Defense
DPO	Defense Privacy Office
FOIA	Freedom of Information Act
FOID	Freedom of Information Division
IAW	In Accordance With
OGC	Office of General Counsel
OIG	Office of Inspector General
PA	Privacy Act
POC	Point of Contact
SSN	Social Security Number