Department of Defense
DIRECTIVE

NUMBER 5400.11
May 8, 2007

DA&M

SUBJECT: DoD Privacy Program

References: (a) DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004 (hereby canceled)
(b) Section 552a of title 5, United States Code
(c) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996
(d) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(e) through (m), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues Reference (a) to update the policies and responsibilities of the DoD Privacy Program under References (b) and (c).

1.2. Authorizes the Defense Privacy Board, the Defense Privacy Board Legal Committee, and the Defense Data Integrity Board.

1.3. Continues to authorize the publication of Reference (d).

1.4. Continues to delegate authorities and responsibilities for the effective administration of the DoD Privacy Program.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector

General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereinafter referred to collectively as the "DoD Components").

2.2. Shall be made applicable to DoD contractors who are operating a system of records on behalf of a DoD Component, to include any of the activities associated with maintaining a system of records, such as collecting and disseminating records.

3. DEFINITIONS

Terms used in this Directive are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The privacy of an individual is a personal and fundamental right that shall be respected and protected.

4.1.1. The DoD'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 against unwarranted invasions of their privacy.

4.1.2. The legal rights of individuals, as guaranteed by Federal laws, regulations, and policies, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals.

4.1.3. DoD personnel, to include contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual.

4.1.4. DoD legislative, regulatory, or other policy proposals shall be evaluated to ensure that privacy implications, including those relating to the collection, maintenance, use, or dissemination of personal information, are assessed, to include, when required and consistent with section 3501of 44 United States Code (U.S.C.) (Reference (e)), the preparation of a Privacy Impact Assessment.

4.2. Personal information shall be collected, maintained, used, or disclosed to ensure that:

4.2.1. It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statutes or Executive orders.

4.2.2. It shall be collected to the greatest extent practicable directly from the individual. The individual shall be informed as to why the information is being collected, the authority for

collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

4.2.3. It shall be relevant, timely, complete, and accurate for its intended use. Appropriate administrative, technical, and physical safeguards shall be established, based on the media (paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage, transfer, or use, including working at authorized alternative worksites.

4.3. No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

4.3.1. When specifically authorized by statute.

4.3.2. When expressly authorized by the individual on whom the record is maintained.

4.3.3. When the record is pertinent to and within the scope of an authorized law enforcement activity.

4.4. Notices shall be published in the Federal Register, and reports shall be submitted to Congress and the Office of Management and Budget (OMB), in accordance with and as required by References (b) through (d), as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, used, or disseminated until the required publication and review requirements, as set forth in References (b) through (d), are satisfied.

4.5. Individuals shall be permitted, to the extent authorized by References (b) and (d), to:

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

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

4.5.3. Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete.

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

4.6. Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by Reference (b), Reference (d), and DoD 5400.7-R (Reference (f)). When disclosures are made, the individual shall be permitted, to the extent authorized by References (b) and (d), to seek an accounting of such disclosures from the DoD Component making the release.

4.7. Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency shall be prohibited to the extent authorized by Public Law 86-36 (1959) and

10 U.S.C. 424 (References (g) and (h)), respectively. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to the extent authorized by section 130b of Reference (h). Disclosure of medical records is prohibited except as authorized by DoD 6025.18-R (Reference (i)).

4.8. Computer matching programs between the DoD Components and Federal, or local governmental agencies shall be conducted in accordance with the requirements of References (b) through (d).

4.9. DoD personnel and system managers shall conduct themselves consistent with established rules of conduct (see Enclosure 3), so that personal information to be stored in a system of records shall only be collected, maintained, used, and disseminated, as authorized by this Directive and References (b) and (d).

4.10. DoD personnel, including but not limited to family members, retirees, contractors, and volunteers, shall be notified in a timely manner, consistent with the requirements of Reference (d), if their personal information, whether or not included in a system of records, is lost, stolen, or compromised.

4.11. DoD Field Activities shall receive administrative support for their DoD Privacy Programs from the Director, Washington Headquarters Services (WHS).

5. RESPONSIBILITIES

5.1. The Director of Administration and Management (DA&M) shall:

5.1.1. Serve as the Senior Privacy Official for the Department of Defense.

5.1.2. Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in References (b) and (c).

5.1.3. Publish Reference (d) and other guidance, to include Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

5.1.4. Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (see Enclosure 4).

5.1.5. Supervise and oversee the activities of the Defense Privacy Office (see Enclosure 4).

5.2. The Director, WHS, under the authority, direction, and control of the DA&M, shall provide DoD Privacy Program support for DoD Field Activities.

5.3. The General Counsel of the Department of Defense (GC, DoD) shall:

5.3.1. Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the DoD Privacy Program.

5.3.2. Review and be the final approval authority on all advisory opinions issued by the Defense Privacy Board or the Defense Privacy Board Legal Committee.

5.3.3. Serve as a member of the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee (see Enclosure 4).

5.4. The Secretaries of the Military Departments and the Heads of the DoD Components, except as noted in paragraph 4.11., shall:

5.4.1. Provide adequate funding and personnel to establish and support an effective DoD Privacy Program, to include the appointment of a senior official to serve as the principal point of contact (POC) for DoD Privacy Program matters.

5.4.2. Establish procedures as well as rules of conduct necessary to implement this Directive and Reference (d) to ensure compliance with the requirements of References (b) and (c).

5.4.3. Conduct training, consistent with the requirements of Reference (d), on the provisions of this Directive and References (b) through (d), for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DoD Privacy Program.

5.4.4. Ensure that all DoD Component legislative proposals, policies, or programs having privacy implications, such as the DoD Privacy Impact Assessment Program (Reference (e)), are evaluated to ensure consistency with the information privacy principles of this Directive and Reference (d).

5.4.5. Assess the impact of technology on the privacy of personal information and, when feasible, adopt privacy-enhancing technology both to preserve and protect personal information contained in DoD Component systems of record and to permit auditing of compliance with the requirements of this Directive and Reference (d).

5.4.6. Ensure that the DoD Component Privacy Program periodically shall be reviewed by the IGs, or other officials, who shall have specialized knowledge of the DoD Privacy Program.

5.4.7. Submit reports, consistent with the requirements of Reference (d), as mandated by References (b) and (c), and DoD Directive 5500.1 (Reference (j)), and as otherwise directed by the Defense Privacy Office.

5.5. The Secretaries of the Military Departments shall provide support to the Combatant Commands, as identified in DoD Directive 5100.3 (Reference (k)), in the administration of the DoD Privacy Program.

6. INFORMATION REQUIREMENTS

The reporting requirements in subparagraph 5.4.7., are assigned Report Control Symbol DD-DA&M(A)1379, in accordance with DoD 8910.1-M (Reference (l)).

7. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 4

E1. References, continued
E2. Definitions
E3. Rules of Conduct
E4. Privacy Boards and Office Composition and Responsibilities

E1. ENCLOSURE 1

REFERENCES, continued

(e) Section 3501 of title 44, United States Code, Note (Section 208, "Privacy Provisions," E-Government Act of 2002)
(f) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(g) Public Law 86-36, "National Security Agency-Officers and Employees," May 29, 1959
(h) Sections 130b and 424 of title 10, United States Code
(i) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
(j) DoD Directive 5500.1, "Processing of Legislation, Executive Orders, Proclamations, and Comments thereon," May 21, 1964
(k) DoD Directive 5100.3, "Support of the Headquarters of the Combatant and Subordinate Joint Commands," January 5, 2006
(l) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
(m) Section 3544(c) of title 44, United States Code

E2. ENCLOSURE 2

DEFINITIONS

E2.1. 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, except as otherwise provided in Reference (d). Members of the United States 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 Department of Defense, but persons employed by such organizations or entities are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits).

E2.2. 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 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 which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; 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.

E2.3. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic), 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 fingerprint, a voice print, or a photograph.

E2.4. System Manager. The DoD Component official who is responsible for the operation and management of a system of records.

E2.5. System of Records. A group of records under the control of a DoD Component 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.

E3. ENCLOSURE 3

RULES OF CONDUCT

E3.1. DoD personnel shall:

E3.1.1. Take such actions, as considered appropriate, to ensure that any personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.

E3.1.2. Not disclose any personal information contained in any system of records, except as authorized by Reference (d), or other applicable laws or regulations. Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

E3.1.3. Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this Directive to the applicable Privacy POC for his or her DoD Component.

E3.2. DoD system managers for each system of records shall:

E3.2.1. Ensure that all personnel who either shall have access to the system of records or who shall 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 DoD Privacy Program.

E3.2.2. Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through their DoD Component Privacy POC to the Defense Privacy Office for publication in the Federal Register.

E3.2.3. Not maintain any official files on individuals, which are retrieved by name or other personal identifier, without first ensuring that a notice for the 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 References (b) through (d), is subject to possible criminal penalties and/or administrative sanctions.

E4. ENCLOSURE 4

PRIVACY BOARDS AND OFFICE COMPOSITION AND RESPONSIBILITIES

E4.1. THE DEFENSE PRIVACY BOARD

E4.1.1. Membership. The Board shall consist of the DA&M, who shall serve as the Chair; the Director of the Defense Privacy Office, DA&M, who shall serve as the Executive Secretary and as a member; the representatives designated by the Secretaries of the Military Departments; and the following officials or their designees: the Deputy Under Secretary of Defense for Program Integration (DUSD(PI)); the Assistant Secretary of Defense for Health Affairs; the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO); the Director, Executive Services Directorate, WHS; the GC, DoD; and the Director, Information Technology Management Directorate (ITMD), WHS. The designees also may be the principal POCs for DoD Component for privacy matters.

E4.1.2. Responsibilities

E4.1.2.1. The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure that the policies, practices, and procedures of that Program are premised on the requirements of References (b) and (c), as well as other pertinent authority, and that the Privacy Programs of the DoD Component are consistent with, and in furtherance of, the DoD Privacy Program.

E4.1.2.2. The Board shall serve as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary, to address issues of common concern so as to ensure that uniform and consistent policy shall be adopted and followed by the DoD Components. The Board shall issue advisory opinions, as necessary, on the DoD Privacy Program to promote uniform and consistent application of References (b) through (d).

E4.1.2.3. Perform such other duties as determined by the Chair or the Board.

E4.2. THE DEFENSE DATA INTEGRITY BOARD

E4.2.1. Membership. The Board shall consist of the DA&M, who shall serve as the Chair; the Director of the Defense Privacy Office, DA&M, who shall serve as the Executive Secretary; and the following officials or their designees: the representatives designated by the Secretaries of the Military Departments; the DUSD(PI); the ASD(NII)/DoD CIO; the GC, DoD; the IG DoD, who shall be a non-voting/advisory member; the Director, ITMD, WHS; and the Director, Defense Manpower Data Center. The designees also may be the principal POCs for the DoD Component for privacy matters.

E4.2.2. Responsibilities

E4.2.2.1. The Board shall oversee and coordinate, consistent with the requirements of References (b) through (d), all computer matching programs involving personal records contained in systems of records maintained by the DoD Components.

E4.2.2.2. The Board shall review and approve all computer matching agreements between the Department of Defense and other Federal, or local governmental agencies, as well as memoranda of understanding, when the match is internal to the Department of Defense, to ensure that, under Reference (b) and References (c) and (d), appropriate procedural and due process requirements shall have been established before engaging in computer matching activities.

E4.3. THE DEFENSE PRIVACY BOARD LEGAL COMMITTEE

E4.3.1. Membership. The Committee shall consist of the Director, Defense Privacy Office, DA&M, who shall serve as the Chair and the Executive Secretary; the GC, DoD, or designee; and civilian and/or military counsel from each of the DoD Components. The GCs and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. That does not preclude representation from each office. The GCs of the other DoD Components shall provide legal representation to the Committee. Other DoD civilian or military counsel may be appointed by the Executive Secretary, after coordination with the DoD Component concerned, to serve on the Committee on those occasions when specialized knowledge or expertise shall be required.

E4.3.2. Responsibilities

E4.3.2.1. The Committee shall serve as the primary legal forum for addressing and resolving all legal issues arising out of or incident to the operation of the DoD Privacy Program.

E4.3.2.2. The Committee shall consider legal questions regarding the applicability of References (b) through (d) and questions arising out of, or as a result of, other statutory and regulatory authority, to include the impact of judicial decisions, on the DoD Privacy Program. The Committee shall provide advisory opinions to the Defense Privacy Board and, on request, to the DoD Components.

E4.4. THE DEFENSE PRIVACY OFFICE

E4.4.1. Membership. It shall consist of a Director and a staff. The Director shall also serve as the Executive Secretary and a member of the Defense Privacy Board; as the Executive Secretary to the Defense Data Integrity Board; and as the Chair and the Executive Secretary to the Defense Privacy Board Legal Committee.

E4.4.2. Responsibilities

E4.4.2.1. Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

E4.4.2.2. Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

E4.4.2.3. Direct the day-to-day activities of the DoD Privacy Program.

E4.4.2.4. Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

E4.4.2.5. Review DoD legislative, regulatory, and other policy proposals which implicate information privacy issues relating to the Department's collection, maintenance, use, or dissemination of personal information, to include any testimony and comments having such implications under Reference (j).

E4.4.2.6. Review proposed new, altered, and amended systems of records, to include submission of required notices for publication in the Federal Register and, when required, providing advance notification to OMB and Congress, consistent with References (b) through (d).

E4.4.2.7. Review proposed DoD Component privacy rulemaking, to include submission of the rule to the Office of the Federal Register for publication and providing to the OMB and the Congress reports, consistent with References (b) through (d).

E4.4.2.8. Develop, coordinate, and maintain all DoD computer matching agreements, to include the submission of required match notices for publication in the Federal Register and the provision of advance notification to OMB and Congress, consistent with References (b) through (d).

E4.4.2.9. Provide advice and support to the DoD Components to ensure that:

E4.4.2.9.1. All information requirements developed to collect or maintain personal data conform to DoD Privacy Program standards.

E4.4.2.9.2. Appropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic or non-electronic means.

E4.4.2.9.3. Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

E4.4.2.10. Serve as the principal POC for coordination of privacy and related matters with the OMB and other Federal, State, and local governmental agencies.

E4.4.2.11. Compile and submit the "Biennial Matching Activity Report" to the OMB in accordance with References (c) and (d) and the Quarterly and Annual Federal Information Security Management Agency (FISMA) Privacy Reports (Reference (m)) and such other reports, as required.

E4.4.2.12. Update and maintain this Directive and Reference (d).