

§ 310.1

32 CFR Ch. I (7–1–11 Edition)

SOURCE: 72 FR 18758, Apr. 13, 2007, unless otherwise noted.

Subpart A—DoD Policy

§ 310.1 Reissuance.

This part consolidates into a single location (32 CFR part 310) Department of Defense (DoD) policies and procedures for implementing the Privacy Act of 1974, as amended (5 U.S.C. 552a) by authorizing the development, publication and maintenance of the DoD Privacy Program set forth by DoD Directive 5400.11¹ and 5400.11–R,² both entitled: “DoD Privacy Program.”

§ 310.2 Purpose.

This part:

(a) Updates policies and responsibilities of the DoD Privacy Program under 5 U.S.C. 552a and OMB Circular A–130.

(b) Authorizes the Defense Privacy Board, the Defense Privacy Board Legal Committee, and the Defense Data Integrity Board.

(c) Continues to authorize the publication of DoD 5400.11–R.

(d) Continues to delegate authorities and responsibilities for the effective administration of the DoD Privacy Program.

§ 310.3 Applicability and scope.

This part:

(a) Applies to the Office of the Secretary of Defense (OSD), 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”).

(b) 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, such as collecting and disseminating records, associated with maintaining a system of records.

(c) This part does not apply to:

(1) Requests for information made under the Freedom of Information Act. They are processed in accordance with DoD 5400.7–R.³

(2) Requests for information from systems of records controlled by the Office of Personnel Management (OPM), although maintained by a DoD Component. These are processed in accordance with policies established by OPM “Privacy Procedures for Personnel Records” (5 CFR 297).

(3) Requests for personal information from the General Accounting Office. These are processed in accordance with DoD Directive 7650.1.⁴

(4) Requests for personal information from Congress. These are processed in accordance with DoD Directive 5400.4 except those specific provisions in Subpart E—Disclosure of Personal Information to Other Agencies and Third Parties.

§ 310.4 Definitions.

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

(b) *Agency.* For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the Department of Defense 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 release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of the Privacy Act.

(c) *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.

(d) *Confidential source.* A person or organization who has furnished information to the Federal Government under an express promise, if made on or after September 27, 1975, that the person’s or the organization’s identity shall be held in confidence or under an implied promise of such confidentiality if this

¹Copies may be obtained at <http://www.dtic.mil/whs/directives>.

²See footnote 1 to § 310.1.

³See footnote 1 to § 310.3(c)(1).

⁴See footnote 1 to § 310.3(c)(1).

implied promise was made on or before September 26, 1975.

(e) *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.

(f) *Federal benefit program.* A program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

(g) *Federal personnel.* Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits).

(h) *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. 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 are "individuals" otherwise (e.g., security clearances, entitlement to DoD privileges or benefits, etc.).

(i) *Individual access.* Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

(j) *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 an other than authorized purpose where one or more individuals will be adversely affected.

Such incidents also are known as *breaches*.

(k) *Maintain.* To maintain, collect, use, or disseminate records contained in a system of records.

(l) *Non-Federal agency.* Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a computer matching program.

(m) *Official use.* Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated a need for the record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R.⁵

(n) *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 also is 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).

(o) *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.

(p) *Member of the public.* Any individual or party acting in a private capacity to include Federal employees or military personnel.

(q) *Recipient agency.* Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a computer matching program.

(r) *Record.* Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic,

⁵ See footnote 1 to § 310.1.

§ 310.5

32 CFR Ch. I (7-1-11 Edition)

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.

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

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

(u) *Source agency.* Any agency which 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.

(v) *Statistical record.* A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(w) *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.

§ 310.5 Policy.

It is DoD policy that:

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

(1) The Department'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.

(2) The legal rights of individuals, as guaranteed by Federal law, regulation, and policy, shall be protected when collecting, maintaining, using, or disseminating personal information about individuals.

(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) Departmental 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 the Privacy Provision of the E-Government Act of 2002 (44 U.S.C. 3501, Note), the preparation of a Privacy Impact Assessment.

(b) Personal information shall be collected, maintained, used, or disclosed to ensure that:

(1) It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statute or Executive order.

(2) It shall be collected to the greatest extent practicable directly from the individual.

(3) 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) It shall be relevant, timely, complete, and accurate for its intended use; and

(5) Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., 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.

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

(1) When specifically authorized by statute;

(2) When expressly authorized by the individual on whom the record is maintained; or

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

(d) Notices shall be published in the FEDERAL REGISTER and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by, 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, 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 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, are satisfied.

(e) Individuals shall be permitted, to the extent authorized by 5 U.S.C. 552a and DoD 5400.11-R, to:

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

(2) Gain access to such records and obtain a copy of those records or a part thereof.

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

(4) Appeal a denial of access or a request for amendment.

(f) 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 5 U.S.C. 552a, DoD 5400.11-R, and DoD 5400.7-R. When disclosures are made, the individual shall be permitted, to the extent authorized by references 5 U.S.C. 552a and/or DoD 5400.11-R, to seek an accounting of such disclosures from the DoD Component making the release.

(g) 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. Disclosure of records pertaining to personnel of overseas, sensitive, or routinely deployable units shall be prohibited to

the extent authorized by 10 U.S.C. 130b. Disclosure of medical records is prohibited except as authorized by DoD 6025.18-R.⁶

(h) Computer matching programs between the DoD Components and the Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(i) DoD personnel and system managers shall conduct themselves consistent with established rules of conduct 310.8 so that personal information to be stored in a system of records only shall be collected, maintained, used, and disseminated as is authorized by this part, 5 U.S.C. 552a and DoD 5400.11-R.

(j) DoD personnel, including but not limited to family members, retirees, contractor employees, and volunteers, shall be notified, in a timely manner, consistent with the requirements of DoD 5400.11-R, if their personal information, whether or not included in a system of records, is lost, stolen, or compromised.

(k) DoD Field Activities shall receive Privacy Program support from the Director, Washington Headquarters Services.

§ 310.6 Responsibilities.

(a) The Director of Administration and Management, Office of the Secretary of Defense, shall:

(1) Serve as the Senior Privacy Official for the Department of Defense.

(2) Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB Circular A-130.

(3) Publish DoD 5400.11-R and other guidance, including Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (see § 310.9).

(5) Supervise and oversee the activities of the Defense Privacy Office (see § 310.9).

⁶See footnote 1 to § 310.1.

§310.7

(b) The Director, WHS, under the DA&M, shall provide Privacy Program support for DoD Field Activities.

(c) The General Counsel of the Department of Defense shall:

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

(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.

(3) Serve as a member of the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee (310.9).

(d) The Secretaries of the Military Departments and the Heads of the Other DoD Components, except as noted in §310.5(k), shall:

(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.

(2) Establish procedures, as well as rules of conduct, necessary to implement this part and DoD 5400.11-R to ensure compliance with the requirements of 5 U.S.C. 552a and OMB Circular A-130.

(3) Conduct training, consistent with the requirements of DoD 5400.11-R, on the provisions of this part, 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, for assigned, employed and detailed, to include contractor, personnel and individuals having primary responsibility for implementing the DoD Privacy Program.

(4) Ensure all Component legislative proposals, policies, or programs having privacy implications, such as the DoD Privacy Impact Assessment Program, are evaluated to ensure consistency with the information privacy principles of this part and DoD 5400.11-R.

(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 Component systems of records and to permit auditing of com-

32 CFR Ch. I (7-1-11 Edition)

pliance with the requirements of this part and DoD 5400.11-R.

(6) Ensure the DoD Privacy Program periodically shall be reviewed by the Inspectors General or other officials, who shall have specialized knowledge of the DoD Privacy Program.

(7) Submit reports, consistent with the requirements of DoD 5400.11-R, as mandated by 5 U.S.C. 552a and OMB Circular A-130, and DoD Directive 5500.1, and as otherwise directed by the DPO.

(e) The Secretaries of the Military Departments shall provide support to the Combatant Commands, as identified in DoD Directive 5100.3,⁷ in the administration of the DoD Privacy Program.

§310.7 Information requirements.

The reporting requirements in §310.6(d)(7) are assigned Report Control Symbol DD-DA&M(A)1379.

§310.8 Rules of conduct.

(a) DoD personnel shall:

(1) Take such actions, as considered appropriate, to ensure that personal information contained in a system of records, to which they have access to 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.

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

(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 part to the applicable Privacy POC for his or her DoD Component.

(b) DoD System Managers for each system of records shall:

(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

⁷ See footnote 1 to §310.1.

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.

(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 DPO for publication in the FEDERAL REGISTER.

(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 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, is subject to possible criminal penalties and/or administrative sanctions.

§ 310.9 Privacy boards and office, composition and responsibilities.

(a) *The Defense Privacy Board*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, 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 (ASD) (NII)/Chief Information Officer (CIO); the Director, Executive Services and Communications Directorate, WHS; the GC, DoD; and the Director for Information Technology Management Directorate (ITMD), WHS. The designees also may be the principal POC for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure the policies, practices, and procedures of that Program are premised on the requirements of 5 U.S.C. 552a and OMB Circular A-130, as well as other pertinent authority, and the Privacy Programs of the DoD Com-

ponent are consistent with, and in furtherance of, the DoD Privacy Program.

(ii) 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 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 so as to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(iii) Perform such other duties as determined by the Chair or the Board.

(b) *The Defense Data Integrity Board*—

(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the DPO, 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)/CIO; the GC, DoD; the Inspector General, DoD; the ITMD, WHS; and the Director, Defense Manpower Data Center. The designees also may be the principal points of contact for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall oversee and coordinate, consistent with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, all computer matching programs involving personal records contained in system of records maintained by the DoD Components.

(ii) The Board shall review and approve all computer matching agreements between the Department of Defense and the other Federal, State or local governmental agencies, as well as memoranda of understanding when the match is internal to the Department of Defense, to ensure, under 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, appropriate procedural and due process requirements shall have been established before engaging in computer matching activities.

(c) *The Defense Privacy Board Legal Committee*—(1) *Membership.* The Committee shall consist of the Director, DPO, 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 General Counsels (GCs) and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. This 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.

(2) *Responsibilities.* (i) 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.

(ii) The Committee shall consider legal questions regarding the applicability of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R 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.

(d) *The DPO—(1) Membership.* It shall consist of a Director and a staff. The Director also shall 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.

(2) *Responsibilities.* (i) Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

(ii) Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

(iii) Direct the day-to-day activities of the DoD Privacy Program.

(iv) Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

(v) 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 DoD Directive 5500.1.

(vi) 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 the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(vii) 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 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(viii) 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 the OMB and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(ix) Provide advice and support to the DoD Components to ensure:

(A) All information requirements developed to collect or maintain personal data conform to DoD Privacy Program standards;

(B) 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; and

(C) Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

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

(xi) Compile and submit the "Biennial Matching Activity Report" to the OMB as required by OMB Circular A-130 and

DoD 5400.11-R, and the Quarterly and Annual Federal Information Security Management Agency (FISMA) Privacy Reports, as required by 44 U.S.C. 3544(c), such other reports as may be required.

(xii) Update and maintain this part and DoD 5400.11-R.

Subpart B—Systems of Records

§ 310.10 General.

(a) *System of Records.* To be subject to the provisions of this part, a “system of records” must:

(1) Consist of “records” (as defined in 310.4(r)) that are retrieved by the name of an individual or some other personal identifier; and

(2) Be under the control of a DoD Component.

(b) *Retrieval practices.* (1) Records in a group of records that MAY be retrieved by a name or personal identifier are not covered by this part even if the records contain personal data and are under control of a DoD Component. The records MUST be retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(i) When records are contained in an automated (Information Technology) system that is capable of being manipulated to retrieve information about an individual, this does not automatically transform the system into a system of records as defined in this part.

(ii) In determining whether an automated system is a system of records that is subject to this part, retrieval policies and practices shall be evaluated. If DoD Component policy is to retrieve personal information by the name or other unique personal identifier, it is a system of records. If DoD Component policy prohibits retrieval by name or other identifier, but the actual practice of the Component is to retrieve information by name or identifier, even if done infrequently, it is a system of records.

(2) If records are retrieved by name or personal identifier, a system notice must be submitted in accordance with § 310.33.

(3) If records are not retrieved by name or personal identifier but then are rearranged in such a manner that

they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with § 310.33.

(4) If records in a system of records are rearranged so that retrieval is no longer by name or other personal identifier, the records are no longer subject to this part and the system notice for the records shall be deleted in accordance with § 310.34.

(c) *Relevance and necessity.* Information or records about an individual shall only be maintained in a system of records that is relevant and necessary to accomplish a DoD Component purpose required by a Federal statute or an Executive Order.

(d) *Authority to establish systems of records.* Identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. The existence of a statute or Executive Order mandating the maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary. If a statute or Executive Order does not expressly direct the creation of a system of records, but the establishment of a system of records is necessary in order to discharge the requirements of the statute or Executive Order, the statute or Executive Order shall be cited as authority.

(e) *Exercise of First Amendment rights.* (1) Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution except when:

(i) Expressly authorized by Federal statute;

(ii) Expressly authorized by the individual; or

(iii) Maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity.

(2) First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.