AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

individually identifiable or use of sampling of certain data for certain individuals only. Additionally, consideration is to be given to the length of time information is needed, and the cost of maintaining the information compared to the risks and adverse consequences of not maintaining the information.

(c) Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(d) Let individuals have access to, and obtain copies of, all or portions of their records, subject to exemption procedures authorized by law and this subpart and subpart G of this part.

(e) Let individuals request amendment of their records when discrepancies proven to be erroneous, untimely, incomplete, or irrelevant are noted.

(f) Let individuals request an administrative review of decisions that deny them access, or refuse to amend their records.

(g) Ensure that adequate safeguards are enforced to prevent misuse, unauthorized disclosure, alteration, or destruction of personal information in records.

(h) Maintain no records describing how an individual exercises his or her rights guaranteed by the First Amendment (freedom of religion, political beliefs, speech, and press; peaceful assemblage; and petition for redress of grievances), unless they are:

(1) Expressly authorized by statute;

(2) Authorized by the individual;

(3) Within the scope of an authorized law enforcement activity; or

(4) For the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains. This should not be construed, however, as restricting or excluding solicitation of information which the individual is willing to have in his or her record concerning religious preference, particularly that required in emergency situations.

(5) Maintain only systems of records which have been published in the FEDERAL REGISTER, in accordance with periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211 and § 701.105. These OPNAVNOTEs 5211 provide a listing of all Department of the Navy Privacy Act systems of records and identify the Office of Personnel Management (OPM) government-wide systems containing information on Department of the Navy civilian employees, even though technically, Department of the Navy does not have cognizance over them. A Privacy Act systems notice outlines what kinds of information may be collected and maintained by naval activities. When collecting/maintaining information in a Privacy Act system of records, review the systems notice to ensure activity compliance is within the scope of the system. If you determine the systems notice does not meet your needs, contact the systems manager or Chief of Naval Operations (N09B30) with your concerns so that amendment of the system may be considered.

§ 701.104 Responsibility and authority.

(a) *Chief of Naval Operations (CNO).* CNO is designated as the official responsible for administering and supervising the execution of 5 U.S.C. 552a, DoD Directive 5400.11, and DoD 5400.11–R. CNO has designated the Assistant Vice Chief of Naval Operations (N09B30) as principal Privacy Act Coordinator for the Department of the Navy to:

(1) Set Department of the Navy policy on the provisions of the Privacy Act.

(2) Serve as principal advisor on all Privacy Act matters.

(3) Oversee the administration of the Privacy Act program, which includes preparing the Department of the Navy Privacy Act report for submission to Congress.

(4) Develop Navy-wide Privacy Act training program and serve as training-oversight manager.

(5) Conduct staff assistance visits within Department of the Navy to review compliance with 5 U.S.C. 552a and this subpart and subpart G of this part.

(6) Coordinate and prepare responses for Privacy Act requests received for Office of the Secretary of the Navy records.

(b) *Commandant of the Marine Corps (CMC).* CMC is responsible for administering and supervising the execution of this subpart and subpart G of this

part within the Marine Corps. The Commandant has designated the Director, Manpower Management Information Systems Division (HQMC (Code MI)) as the Privacy Act coordinator for Headquarters, U.S. Marine Corps.

(c) *Privacy Act Coordinator.* Each addressee is responsible for implementing and administering a Privacy Act program under this subpart and subpart G of this part. Each addressee shall designate a Privacy Act Coordinator to:

(1) Serve as principal point of contact on Privacy Act matters.

(2) Provide training for activity/command personnel on the provisions of 5 U.S.C. 552a and this subpart and subpart G of this part.

(3) Issue implementing instruction which designates the activity's Privacy Act Coordinator, Privacy Act records disposition, Privacy Act processing procedures, identification of Privacy Act systems of records under their cognizance, and training aids for those personnel involved with systems of records.

(4) Review internal directives, practices, and procedures, including those having Privacy Act implications and where Privacy Act Statements (PASs) are needed.

(5) Compile input and submit consolidated Privacy Act report to Echelon 2 Privacy Act Coordinator, who, in turn, will provide consolidated report to CNO (N09B30).

(6) Maintain liaison with records management officials (i.e., maintenance and disposal procedures and standards, forms, and reports), as appropriate.

(7) Provide guidance on handling Privacy Act requests and scope of Privacy Act exemptions.

(8) Conduct staff assistance visits within command and lower echelon commands to ensure compliance with the Privacy Act.

(9) Echelon 2 Privacy Act Coordinators shall provide CNO (N09B30) with a complete listing of all Privacy Act Coordinators under their jurisdiction. Such information should include activity name and address, office code, name of Privacy Act Coordinator, commercial and DSN telephone number, and FAX number, if applicable.

(d) *Release authority.* Officials having cognizance over the requested subject matter are authorized to respond to requests for notification, access, and/or amendment of records. These officials could also be systems managers (see § 701.104(g)).

(e) *Denial authority.* Within the Department of the Navy, the following chief officials, their respective vice commanders, deputies, principal assistants, and those officials specifically designated by the chief official are authorized to deny requests, either in whole or in part, for notification, access and amendment, made under this subpart and subpart G of this part, when the records relate to matters within their respective areas of responsibility or chain of command:

(1) *Department of the Navy.* Civilian Executive Assistants; CNO; CMC; Chief of Naval Personnel; Commanders of the Naval Systems Commands, Office of Naval Intelligence, Naval Security Group Command, Naval Imaging Command, and Naval Computer and Telecommunications Command; Chief, Bureau of Medicine and Surgery; Auditor General of the Navy; Naval Inspector General; Director, Office of Civilian Personnel Management; Chief of Naval Education and Training; Commander, Naval Reserve Force; Chief of Naval Research; Commander, Naval Oceanography Command; heads of Department of the Navy Staff Offices, Boards, and Councils; Flag Officers and General Officers. NJAG and his Deputy, and OGC and his Deputies are excluded from this grant of authorization. While NJAG and OGC are not denial authorities, they are authorized to further delegate the authority conferred here to other senior officers/officials within NJAG and OGC.

(2) *For the shore establishment.*(i) All officers authorized under Article 22, Uniform Code of Military Justice (UCMJ) or designated in section 0120, Manual of the Judge Advocate General (JAGINST 5800.7C)[5], to convene general courts-martial.

(ii) Commander, Naval Investigative Service Command.

[5] Copies available from the Judge Advocate General, Navy Department, 200 Stovall Street, Alexandria, VA 22332–2400.

(iii) Deputy Commander, Naval Legal Service Command.

(3) *In the Operating Forces.* All officers authorized by Article 22, Uniform Code of Military Justice (UCMJ), or designated in section 0120, Manual of the Judge Advocate General (JAGINST 5800.7C), to convene general courts-martial.

(f) *Review authority.* (1) The Assistant Secretary of the Navy (Manpower and Reserve Affairs), is the Secretary's designee, and shall act upon requests for administrative review of initial denials of requests for amendment of records related to fitness reports and performance evaluations of military personnel (see § 701.111(c)(3)).

(2) The Judge Advocate General and General Counsel, as the Secretary's designees, shall act upon requests for administrative review of initial denials of records for notification, access, or amendment of records, as set forth in § 701.111(c)(2) and (4).

(3) The authority of the Secretary of the Navy (SECNAV), as the head of an agency, to request records subject to the Privacy Act from an agency external to the Department of Defense for civil or criminal law enforcement purposes, under subsection (b)(7) of 5 U.S.C. 552a, is delegated to the Commandant of the Marine Corps, the Director of Naval Intelligence, the Judge Advocate General, and the General Counsel.

(g) *Systems manager.* Systems managers, as designated in Department of the Navy's compilation of systems notices (periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211[6], ''Current Privacy Act Issuances'') shall:

(1) Ensure the system has been published in the FEDERAL REGISTER and that any additions or significant changes are submitted to CNO (N09B30) for approval and publication. The systems of records should be maintained in accordance with the systems notices as published in the periodic Chief of Naval Operations Notes (OPNAVNOTEs) 5211, ''Current Privacy Act Issuances.''

(2) Maintain accountability records of disclosures.

[6] See footnote 3 to § 701.101.

(h) *Department of the Navy employees.* Each employee of the Department of the Navy has certain responsibilities for safeguarding the rights of others. These include:

(1) Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this subpart and subpart G of this part.

(2) Not maintaining unpublished official files which would fall under the provisions of 5 U.S.C. 552a.

(3) Safeguarding the privacy of individuals and confidentiality of personal information contained in a system of records.

§ 701.105 Systems of records.

To be subject to this subpart and subpart G of this part, a ''system of records'' must consist of ''records'' that are retrieved by the name, or some other personal identifier, of an individual and be under the control of Department of the Navy.

(a) *Retrieval practices.* (1) Records in a group of records that are not retrieved by personal identifiers are not covered by this subpart and subpart G of this part, even if the records contain information about individuals and are under the control of Department of the Navy. The records must be retrieved by personal identifiers to become a system of records.

(2) If records previously not retrieved by personal identifiers are rearranged so they are retrieved by personal identifiers, a new system notice must be submitted in accordance with § 701.107.

(3) If records in a system of records are rearranged so retrieval is no longer by personal identifiers, the records are no longer subject to this subpart and subpart G of this part and the records system notice should be deleted in accordance with § 701.107.

(b) *Recordkeeping standards.* A record maintained in a system of records subject to this subpart and subpart G of this part must meet the following criteria:

(1) Be accurate. All information in the record must be factually correct.

(2) Be relevant. All information contained in the record must be related to the individual who is the record subject