

## Office of the Secretary of Defense

## § 326.5

corporate information such as name, work telephone number, and position. Good recordkeeping practices dictate that only rosters that are relevant and necessary to the NRO's operations may be maintained, and therefore convenience rosters, which by definition do not satisfy the test, may not be maintained.

### § 326.5 Responsibilities.

(a) The Director, NRO (DNRO):

(1) Supervises the execution of the Privacy Act and this part within the NRO.

(2) Appoints:

(i) The Chief, Information Access and Release Center as the NRO Privacy Act Coordinator.

(ii) The Director of Security, the Director of Policy, and the NRO General Counsel as the NRO Appeals Panel; and

(iii) The Chief of Staff as the Senior Official for Privacy Policy and the Privacy Act Appeal Authority.

(b) The Privacy Act Coordinator, NRO:

(1) Establishes, issues, and updates policy for the NRO Privacy Act Program, monitors compliance, and serves as the principal NRO point of contact on all Privacy Act matters.

(2) Receives, processes, and responds to all Privacy Act requests received by the NRO, including:

(i) Granting, granting in part, or denying an initial Privacy Act request for access or amendment to a record, and notifying a requester of such actions taken in regard to that request.

(ii) Granting a requester access to all or part of a record under dispute when, after a review, a decision is made in favor of a requester.

(iii) Directing the appropriate NRO component to amend a record and advising other record holders to amend a record when a decision is made in favor of a requester.

(iv) Notifying a requester, if a request is denied, of the reasons for denial and the procedures for appeal to the Privacy Act Appeal Authority.

(v) Notifying a requester of his right to file a concise statement of his reasons for disagreement with the NRO's refusal to amend a record.

(vi) Directing that a requester's statement of reasons for the request to

amend, his concise statement of disagreement with the NRO's refusal to amend a record, and the NRO's letter of denial be included in the file containing the disputed record.

(vii) Referring all appeals to the Privacy Act Appeals Panel and Appeal Authority.

(viii) Notifying a requester of any required fees and delivering such collected fees to the Comptroller.

(ix) Obtaining supplemental information from the requester when required.

(3) Serves as the NRO point of contact with the Defense Privacy Office.

(4) Reviews NRO use of records, and at least 40 calendar days prior to establishing a new agency system of records, ensures that new or amended notices are prepared and published in the FEDERAL REGISTER consistent with the requirements of 32 CFR part 310;

(5) Coordinates with forms managers to ensure that a Privacy Act Statement is on all forms or in all other methods used to collect personal information for inclusion in any NRO records system;

(6) Prepares the NRO Privacy Act report for submission to the DoD Privacy Office and to other authorities, as required by 32 CFR part 310.

(7) Reviews all procedures, including forms, which require an individual to furnish information for conformity with the Privacy Act.

(8) Retains the accounting of disclosures for at least five years or for the life of the record, whichever is longer, to be available for review by the subject of the record at his request except for disclosures made under paragraph (c)(7) of § 326.4; and

(9) Develops and oversees Privacy Act Program training for NRO personnel.

(c) The Privacy Act Appeals Panel, NRO:

(1) Meets and reviews all denials appealed by means of the NRO internal appeals process; and

(2) Recommends a finding to the Privacy Act Appeal Authority by a majority vote of those present at the meeting and based on the written record and the panel's deliberations.

(d) The Privacy Act Appeal Authority, NRO:

(1) Determines all NRO Privacy Act appeals.

**§ 326.5**

**32 CFR Ch. I (7-1-10 Edition)**

(2) Reports the determination to the PA Coordinator.

(3) Signs the final appeal letter to the requester.

(e) General Counsel, NRO:

(1) Ensures uniformity in NRO legal positions concerning the Privacy Act and reviews proposed responses to Privacy Act requests to ensure legal sufficiency, as appropriate.

(2) Consults with DoD General Counsel on final denials that may be inconsistent with other final decisions within DoD; raises new legal issues of potential significance to other government agencies.

(3) Provides advice and assistance to the DNRO, the PA Coordinator, and component Directors, as required, in the discharge of their responsibilities pertaining to the Privacy Act.

(4) Advises on all legal matters concerning the Privacy Act, including legal decisions, rulings by the Department of Justice, and actions by DoD and other commissions on the Privacy Act.

(5) Approves all Privacy Act Statements prior to their reproduction and distribution.

(6) Acts as the NRO focal point for Privacy Act litigation with the Department of Justice.

(7) Provides a status report to the Defense Privacy Office, consistent with the requirements of 32 CFR part 310, whenever an individual brings suit under subsection (g) of the Privacy Act against NRO.

(f) Chief Information Officer (CIO), NRO:

(1) Ensures that NRO systems of records databases have procedures to protect the confidentiality of personal records maintained or processed by means of automatic data processing (ADP) systems and ensures that ADP systems contain appropriate safeguards for the privacy of personnel.

(2) Coordinates with the PA Coordinator before developing or modifying CIO-sponsored ADP supported files subject to the provisions of this part.

(g) Directorate and Office Managers, NRO:

(1) Ensure that records contained in their directorate or office systems of records are disclosed only to those

NRO officials or employees who require the records for official purposes.

(2) Review their own directorate and office systems of records to ensure and certify that no systems of records other than those listed in the FEDERAL REGISTER System Notices are maintained; notify the CIO and the PA Coordinator promptly whenever there are changes to processing equipment, hardware, software, or database that may require an amended system notice.

(3) Maintain only such information about an individual as is relevant and necessary to accomplish a purpose which is required by statute or Executive Order and identify the specific provision of law or Executive Order which provides authority for the maintenance of information in each system of records.

(h) System Managers, NRO:

(1) Ensure that adequate safeguards have been established and are enforced to prevent the misuse, unauthorized disclosure, alteration, or destruction of personal information contained in system records.

(2) Ensure that all personnel who have access to the system of records, or are engaged in developing or supervising procedures for handling records, are aware of their responsibilities established by the NRO Privacy Act Program.

(3) Evaluate each system of records during the planning stage and at regular intervals. The following factors should be considered:

(i) Relationship of data to be collected and retained to the purposes for which the system is maintained (all information must be relevant and necessary to the purpose for which it is collected).

(ii) The specific impact on the purpose or mission if categories of information are not collected (all data fields must be necessary to accomplish a lawful purpose or mission).

(iii) Whether informational needs can be met without using personal identifiers.

(iv) The cost of maintaining and disposing of records within the systems of records and the length of time each item of information must be retained according to the NRO Records Control

Schedule as approved by the National Archives and Records Administration.

(4) Review system alterations or amendments to evaluate for relevancy and necessity.

(i) Forms and Information Managers. All NRO individuals responsible for forms or methods used to collect personal information from individuals will:

(1) Ensure that Privacy Act Statements are on appropriate forms and that new forms have the required Privacy Act Statement.

(2) Determine, with General Counsel's concurrence, which forms require Privacy Act Statements and will prepare such statements.

(3) Assist the initiators in determining whether a form, format, questionnaire, or report requires a Privacy Act Statement. Privacy Act Statements must be complete, specific, written in plain English, and approved by the Office of General Counsel.

(j) Employees, NRO:

(1) Will be familiar with the provisions of this part regarding the maintenance of systems of records, authorized access, and authorized disclosure;

(2) Will collect, maintain, use, and/or disseminate records containing identifiable personal information only for lawful purposes; will keep the information current, complete, relevant, and accurate for its intended use; and will safeguard the records in a system and keep them the minimum time required;

(3) Will not disclose any personal information contained in any system of records, except as authorized by the Privacy Act and this part;

(4) Will maintain no system of records concerning individuals except those authorized, and will maintain no other information concerning individuals except as necessary for the conduct of business at the NRO;

(5) Will provide individuals a Privacy Act Statement when asking them to provide information about themselves. The Privacy Act Statement will include the authority under which the information is being requested, whether disclosure of the information is mandatory or voluntary, the purposes for which it is being requested, the uses to which it will be put, and the con-

sequences of not providing the information;

(6) May not deny an individual any right or privilege provided by law because of that individual's failure to disclose his SSN unless such information is required by federal statute or disclosure was required by statute or regulations adopted prior to January 1, 1975. If disclosure of the SSN is not required, NRO directorates and offices are not precluded from requesting it from individuals; however, the Privacy Act Statement must make clear that the disclosure of the SSN is voluntary and, if the individual refuses to disclose it, must be prepared to identify him by alternate means.

(7) Will collect personal information directly from the subject whenever possible; employees may collect information from third parties when that information must be verified, opinions or evaluations are required, the subject cannot be contacted, or the subject requests it.

(8) Will keep paper and electronic records which contain personal information and are retrieved by name or personal identifier only in approved systems published in the FEDERAL REGISTER.

(9) Will amend and correct records when directed by the PA Coordinator.

(10) Will report to the PA Coordinator any disclosures of personal information from a system of records, or the maintenance of any system of records, not authorized by this part.

(11) Will participate in specialized Privacy Act training should their duties require dealing with special investigators, the news media, or the public.

[65 FR 20372, Apr. 17, 2000, as amended at 66 FR 41783, Aug. 9, 2001]

#### **§ 326.6 Policies for processing requests for records.**

(a) An individual's written request for access to records about himself which does not specify the Act under which the request is made will be processed under both the Freedom of Information Act (FOIA) and the Privacy Act and the applicable regulations. Such requests will be processed under both Acts regardless of whether the requester cites one Act, both, or neither in the request in order to ensure the