

be given before a naval activity may begin to collect information for or use a new system of records. The following procedures apply:

(1) Describe in the record system notice the contents of the record system and the purposes and routine uses for which the information will be used and disclosed.

(2) The public shall be given 30 days to comment on any proposed routine uses before the routine uses are implemented.

(3) The notice shall contain the date the system of records will become effective.

(b) *Criteria for an alteration to a system of records notice.* A system is considered altered when any one of the following actions occur or is proposed:

(1) A significant increase or change in the number or types of individuals about whom records are maintained. For example, a decision to expand a system of records that originally covered personnel assigned to only one naval activity to cover personnel at several installations would constitute an altered system. An increase or decrease in the number of individuals covered due to normal growth or decrease is not an alteration.

(2) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would be an alteration.

(3) A change that alters the purpose for which the information is used. In order to be an alteration, the change must be one that is not reasonably inferred from any of the existing purposes.

(4) A change to equipment configuration (either hardware or software) that creates substantially greater use of records in the system. For example, placing interactive computer terminals at regional offices when the system was formerly used only at the headquarters would be an alteration.

(5) A change in the manner in which records are organized or in the method by which records are retrieved.

(6) Combining record systems due to a reorganization within Department of the Navy.

(7) Retrieving by Social Security Numbers (SSNs), records that pre-

viously were retrieved only by names would be an alteration if the present notice failed to indicate retrieval by SSNs. An altered system of records must be published in the FEDERAL REGISTER. Submission for an alteration must contain a narrative statement, the specific changes altering the system, and the system of records notice.

(c) *Criteria for amending a systems of records notice.* Minor changes to published system of records notices are considered amendments. All amendments should be forwarded to CNO (N09B30) for publication in the FEDERAL REGISTER. When submitting an amendment to a system of records notice, the naval activity must include a description of the specific changes proposed and the system of records notice.

(d) *Criteria for deleting a system of records notice.* When a system of records is discontinued, incorporated into another system, or determined to be no longer subject to this subpart and subpart G of this part, a deletion notice must be published in the FEDERAL REGISTER. The deletion notice shall include the system identification number, system name, and the reason for deleting it. If a system is deleted through incorporation into or merger with another system, identify the successor system in the deletion notice.

§ 701.108 Collecting information about individuals.

(a) *Collecting directly from the individual.* To the greatest extent practicable, collect information for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under the Federal programs.

(b) *Collecting information about individuals from third persons.* It might not always be practical to collect all information about an individual directly from that person, such as verifying information through other sources for security or employment suitability determinations; seeking other opinions, such as a supervisor's comments on past performance or other evaluations; obtaining the necessary information directly from the individual would be exceptionally difficult or would result

in unreasonable costs or delays; or, the individual requests or consents to contacting another person to obtain the information.

(c) *Soliciting the social security number (SSN).* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, this prohibition does not apply if a Federal law requires that the SSN be provided, or the SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual must be advised whether providing the SSN is mandatory or voluntary; by what law or other authority the SSN is solicited; and what uses will be made of the SSN.

(3) The preceding advice relates only to the SSN. If other information about the individual is solicited for a system of records, a Privacy Act statement (PAS) also must be provided to him/her.

(4) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether it is mandatory for the individuals to provide their SSNs. E.O. 9397 requires federal agencies to use SSNs as numerical identifiers for individuals in most federal records systems, however, it does not make it mandatory for individuals to provide their SSNs.

(5) When entering military service or civilian employment with the Department of the Navy, individuals must provide their SSNs. This is then the individual's numerical identifier and is used to establish personnel, financial, medical, and other official records (as authorized by E.O. 9397). The individuals must be given the notification described above. Once the individual has provided his or her SSN to establish the records, a notification is not required when the SSN is requested only for identification or to locate the records.

(6) The Federal Personnel Manual⁸ must be consulted when soliciting SSNs for use in systems of records maintained by the Office of Personnel Management.

(7) A Department of the Navy activity may request an individual's SSN even though it is not required by Federal statute, or is not for a system of records in existence and operating prior to January 1, 1975. However, the separate Privacy Act Statement for the SSN, alone, or a merged Privacy Act Statement covering both the SSN and other items of personal information, must make clear that disclosure of the number is voluntary. If the individual refuses to disclose his or her SSN, the activity must be prepared to identify the individual by alternate means.

(d) *Contents of Privacy Act Statement.*

(1) When an individual is requested to furnish information about himself/herself for a system of records, a Privacy Act Statement must be provided to the individual, regardless of the method used to collect the information (i.e., forms, personal or telephonic interview, etc). If the information requested will not be included in a system of records, a Privacy Act Statement is not required.

(2) The Privacy Act Statement shall include the following:

(i) The Federal law or E.O. that authorizes collecting the information (i.e., E.O. 9397 authorizes collection of SSNs);

(ii) Whether or not it is mandatory for the individual to provide the requested information (It is only mandatory when a Federal law or E.O. of the President specifically imposes a requirement to furnish the information and provides a penalty for failure to do so. If furnishing information is a condition for granting a benefit or privilege voluntarily sought by the individual, it is voluntary for the individual to give the information.);

(iii) The principle purposes for collecting the information;

(iv) The routine uses that will be made of the information (i.e., to whom

⁸Copies available from the Office of Personnel Management, 1900 E Street, Washington, DC 20415.

and why it will be disclosed outside the Department of Defense); and

(v) The possible effects on the individual if the requested information is not provided.

(3) The Privacy Act Statement must appear on the form used to collect the information or on a separate form that can be retained by the individual collecting the information. If the information is collected by means other than a form completed by the individual, i.e., solicited over the telephone, the Privacy Act Statement should be read to the individual and if requested by the individual, a copy sent to him/her. There is no requirement that the individual sign the Privacy Act Statement.

(e) *Format for Privacy Act Statement.* When forms are used to collect information about individuals for a system of records, the Privacy Act Statement shall appear as follows (listed in the order of preference):

(1) Immediately below the title of the form,

(2) Elsewhere on the front page of the form (clearly indicating it is the Privacy Act Statement),

(3) On the back of the form with a notation of its location below the title of the form, or

(4) On a separate form which the individual may keep.

§ 701.109 Access to records.

(a) *Individual access to records—* (1) *Right of access.* Only individuals who are subjects of records maintained in systems of records and by whose personal identifiers the records are retrieved have the right of individual access under this subpart and subpart G of this part, unless they provide written authorization for their representative to act on their behalf. Legal guardians or parents acting on behalf of a minor child also have the right of individual access under this subpart and subpart G of this part.

(2) *Notification of record's existence.* Each naval activity shall establish procedures for notifying an individual, in response to his or her request, if a system of records identified by him/her contains a record pertaining to the individual.

(3) *Individual request for access.* Individuals shall address requests for ac-

cess to records in systems of records to the system manager or the office designated in the Department of the Navy compilation of system notices (periodic Chief of Naval Operations Notes (OPNAVNOTES) 5211, "Current Privacy Act Issuances").

(4) *Verifying identity.* (i) An individual shall provide reasonable verification of identity before obtaining access to records.

(ii) When requesting records in writing, naval activities may not insist that a requester submit a notarized signature. The courts have ruled that an alternative method of verifying identity must be established for individuals who do not have access to notary services. This alternative permits requesters to provide an unsworn declaration that states "I declare under perjury or penalty under the laws of the United States of American that the foregoing is true and correct."

(iii) When an individual seeks access in person, identification can be verified by documents normally carried by the individual (i.e., identification card, driver's license, or other license, permit or pass normally used for identification purposes).

(iv) When access is requested other than in writing, identity may be verified by the individual's providing minimum identifying data such as full name, date and place of birth, or other information necessary to locate the record sought. If the information sought is sensitive, additional identifying data may be required. Telephonic requests should not be honored.

(v) Allow an individual to be accompanied by a person of his or her choice when viewing the record; however, require the individual to provide written authorization to have the record discussed in front of the other person.

(vi) Do not deny access to an individual who is the subject of the record solely for refusing to divulge his or her SSN, unless it is the only means of retrieving the record or verifying identity.

(vii) Do not require the individual to explain why he or she is seeking access to a record under this subpart and subpart G of this part.

(viii) Only a designated denial authority may deny access. The denial