

DEPARTMENT OF THE NAVY
Office of the Secretary
Washington, DC 20350-1000

SECNAVINST 5211.5D
OP-09B30
17 July 1992

SECNAV INSTRUCTION 5211.5D

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY
PRIVACY ACT (PA) PROGRAM

- Ref: (a) 5 U.S.C. 552a, as amended by the computer Matching Act of 1988
(b) DOD Directive 5400.11 of 9 Jun 82, DOD Privacy Program (NOTAL)
(c) DOD Regulation 5400.11-R of 31 Aug 83, "DOD Privacy Act Program" (NOTAL)
(d) 5 U.S.C. 552 (1988) as amended by the Freedom of Information Reform Act of 1986
(e) SECNAVINST 5720.42E, Department of the Navy Freedom of Information Act Program
(f) OPM Regulations and the Federal Personnel Manual
(g) 42 U.S.C. 653, Parent Locator Service for Enforcement of Child Support

- Encl: (1) Table of Contents
(2) Contents of Record System Notice and Sample Report on New System of Records Format
(3) Sample Report on Altered System of Records Notice and Format
(4) Contents of an Amended Systems of Records Notice and Format
(5) Contents of a Deleted Systems of Records Notice and Format
(6) Special Considerations for Using and Safeguarding Records in Computerized Systems of Records
(7) Special Considerations for Safeguarding Records during Word Processing
(8) General Purpose Privacy Act Statement (OPNAV 5211/12 (3/92))
(9) DOD Blanket Routine Uses

- (10) Disclosure Accounting Form (OPNAV 5211/9 (3-92))
- (11) List of Exempt Systems
- (12) Sample Exemption Rule
- (13) Provisions of the PA from Which a General or Specific Exemption May Be Claimed
- (14) Litigation Status Report
- (15) Sample Training Package and Slides
- (16) Instructions for Preparing OPNAV Form 5211/10, Annual Report - Privacy Act
- (17) Sample Checklist for Conducting PA Staff Assistance Visits
- (18) Computer Matching Guidelines
- (19) Text of Privacy Act of 1974 (As Amended) - 5 U.S.C. 552a

1. Purpose

a. To provide Department of the Navy (DON) policies and procedures for:

- (1) Governing the collection, safeguarding, maintenance, use, access, amendment, and dissemination of personal information kept by DON in systems of records;
- (2) Notifying individuals if any systems of records contain a record pertaining to them;
- (3) Verifying the identity of individuals who request their records before the records are made available to them;
- (4) Notifying the public of the existence and character of each system of records.
- (5) Exempting systems of records from certain requirements of the PA; and
- (6) Governing the PA rules of conduct for DON personnel, who will be subject to criminal penalties for noncompliance with reference (a).

0579L00559740



b. To implement references (a), (b), and (c), and promote uniformity in DON Privacy Act (PA) Program. This instruction is published in 32 C.F.R. Part 701, subparts F and G.

This instruction is a complete revision and should be read in its entirety. Enclosure (1) is a Table of Contents for this instruction.

2. **Cancellation.** SECNAVINST 5211.5C and Report Control Symbol OPNAV 5211.9.

3. **Applicability**

a. This instruction applies throughout DON. It is also applicable to contractors by contract or other legally binding action, whenever a DON contract provides for the operation of a system of records or portion of a system of records to accomplish a DON function. For the purposes of any criminal liabilities adjudged, any contractor or any employee of such contractor is considered to be an employee of DON.

b. In case of a conflict, this instruction takes precedence over any existing DON directive that deals with the personal privacy and rights of individuals regarding their personal records, except for disclosure of personal information required by reference (d) and implemented by reference (e).

4. **Definitions.** For the purposes of this instruction, the following meanings apply.

a. **Access.** The review or copying of a record or parts thereof contained in a system of records by any individual.

b. **Agency.** For the purposes of disclosing records subject to the PA between or among Department of Defense (DOD) components, DOD is considered a single agency. For all other purposes, DoN is considered an agency within the meaning of PA.

c. **Confidential Source.** A person or organization who has furnished information to the Federal Government either under an express promise that the person's or the organization's

identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

d. **Defense Data Integrity Board.** Consists of members of the Defense Privacy Board, as outlined in reference (b), and, in addition, the DOD Inspector General or the designee, when convened to oversee, coordinate and approve or disapprove all DOD component computer matching covered by the PA.

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

g. **Individual.** A living citizen of the United States or alien lawfully admitted to the U.S. for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a deceased person under this instruction and the term "individual" does not embrace an individual acting in a non-personal capacity (for example, sole proprietorship or partnership).

h. **Individual Access.** Access to information pertaining to the individual by the individual or his/her designated agent or legal guardian.

i. **Maintain.** Includes maintain, collect, use, or disseminate.

j. Member of the Public. Any individual or party acting in a private capacity.

k. Minor. Under this instruction, a minor is an individual under 18 years of age, who is not a member of the U.S. Navy or Marine Corps, nor married.

l. Official Use. Within the context of this instruction, this term is used when DON officials and employees have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties.

m. Personal Information. Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

n. Privacy Act (PA) 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.

o. Record. Any item, collection, or grouping of information about an individual that is maintained by a naval activity including, but not limited to, the individual's education, financial transactions, and medical, criminal, or employment history, and that contains the individual's name or other identifying particulars assigned to the individual, such as a finger or voice print or a photograph.

p. Review Authority. An official charged with the responsibility to rule on administrative appeals of initial denials of requests for notification, access, or amendment of records. The Secretary of the Navy has delegated his review authority to the Assistant Secretary of the Navy (Manpower and Reserve Affairs (ASN (M&RA))), the General Counsel (OGC), and the Judge Advocate General (NJAG). (See paragraph 13). Additionally, the Office of

Personnel Management (OPM) is the review authority for civilian official personnel folders or records contained in any other OPM record.

q. Risk Assessment. An analysis which considers information sensitivity, vulnerability, and cost to a computer facility or word processing center in safeguarding personal information processed or stored in the facility or center.

r. Routine Use. Disclosure of a record outside DOD for a purpose that is compatible with the purpose for which the record was collected and maintained by DOD. The routine use must have been included in the notice for the system of records published in the Federal Register.

s. Statistical Record. A record maintained only for statistical research, or reporting purposes, and not used in whole or in part in making any determination about a specific individual.

t. System Manager. An official who has overall responsibility for a system of records. He/she may serve at any level in DON. Systems managers are indicated in the published record systems notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity). (See paragraph 6g for responsibilities of a system manager).

u. System of Records. A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all PA systems of records must be published in the Federal Register and are also published in periodic OPNAVNOTES 5211, subj: CURRENT PA ISSUANCES.

v. Word Processing Equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, hard wiring,

or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device.

w. **Word Processing System.** A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written communications into a form suitable to the originator. The results are written or graphic presentations intended to communicate verbally or visually with another individual.

x. **Working Day.** All days excluding Saturday, Sunday, and legal holidays.

5. **Policy.** It is the policy of DON to:

a. Ensure that all its personnel comply fully with references (a), (b), and (c) to protect individuals from unwarranted invasions of privacy. Individuals covered by this protection are living citizens of the U.S. or aliens lawfully admitted for permanent residence. A legal guardian of an individual or parent of a minor when acting on the individual's or minor's behalf, has the same rights as the individual or minor. (A member of the Armed Forces is not a minor for the purposes of this instruction.)

b. Collect, maintain, and use only that personal information needed to support a Navy function or program as authorized by law or Executive Order (E.O.), and disclose this information only as authorized by reference (a) and this instruction. In assessing need, consideration shall be given to alternatives, such as use of information not 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 instruction.

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/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/her record concerning religious preference, particularly that required in emergency situations.

i. Maintain only systems of records which have been published in the Federal Register, in accordance with periodic OPNAVNOTEs 5211,

Subj: CURRENT PA ISSUANCES, and paragraph 7. These OPNAVNOTEs 5211 provide a listing of all DON PA systems of records and identify the Office of Personnel Management (OPM) government-wide systems containing information on DON civilian employees, even though technically, DON does not have cognizance over them. A PA systems notice outlines what kinds of information may be collected and maintained by naval activities. When collecting/maintaining information in a PA 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 (CNO) (OP-09B30) with your concerns so that amendment of the system may be considered.

6. Responsibility and Authority

a. CNO. CNO is designated as the official responsible for administering and supervising the execution of references (a), (b), and (c). CNO has designated the Assistant Vice Chief of Naval Operations (OP-09B30) as principal PA Coordinator for the DON to:

- (1) Set DON policy on the provisions of the PA.
- (2) Serve as principal advisor on all PA matters.
- (3) Oversee the administration of the PA program, which includes preparing the DON PA report for submission to Congress.
- (4) Develop Navy-wide PA training program and serve as training-oversight manager.
- (5) Conduct staff assistance visits within DON to review compliance with reference (a) and this instruction.
- (6) Coordinate and prepare responses for PA 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 instruction within the Marine Corps. The Commandant has designated the Director, Manpower Management Information Systems Division (HQMC (Code MI)) as the PA coordinator for Headquarters, U.S. Marine Corps.

c. PA Coordinator. Each addressee is responsible for implementing and administering a PA program under this instruction. Each addressee shall designate a PA Coordinator to:

- (1) Serve as principal point of contact on PA matters.
- (2) Provide training for activity/command personnel on the provisions of reference (a) and this instruction.
- (3) Issue implementing instruction which designates the activity's PA Coordinator, PA records disposition, PA processing procedures, identification of PA 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 PA implications and where Privacy Act Statements (PASSs) are needed.
- (5) Compile input and submit consolidated PA report to Echelon 2 PA Coordinator, who, in turn, will provide consolidated report to CNO (OP-09B30).
- (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 PA requests and scope of PA exemptions.

(8) Conduct staff assistance visits within command and lower echelon commands to ensure compliance with the PA. (See paragraph 19 for conducting staff assistance visits).

(9) Echelon 2 PA Coordinators shall provide CNO (OP-09B30) with a complete listing of all PA Coordinators under their jurisdiction. Such information should include activity name and address office code, name of PA 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 paragraph 6g).

e. Denial Authority. Within DON, 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 instruction, when the records relate to matters within their respective areas of responsibility or chain of command:

(1) DON: Civilian Executive Assistants; CNO; CMC; Chief of Naval Personnel; Commanders of the Naval Systems Commands, Naval Intelligence Command, 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 DON 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:

(a) 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), to convene general courts-martial.

(b) Commander, Naval Investigative Service Command.

(c) Deputy Commander, Naval Legal Service Command.

(3) In the Operating Forces: All officers authorized by Article 22, 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 paragraph 13c(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 paragraphs 13c(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 PA from an agency external to DOD for civil or criminal law enforcement purposes, under subsection (b)(7) of reference (a), is delegated to the Commandant of the Marine Corps, the Director of Naval Intelligence, the Judge Advocate General, and the General Counsel.

g. System Manager. Systems managers, as designated in DON's compilation of systems notices (periodic OPNAVNOTEs 5211, subj: CURRENT PA ISSUANCES) shall:

(1) Ensure the system has been published in the Federal Register and that any additions or significant changes are submitted to CNO (OP-09B30) for approval and publication. The systems of records should be maintained in accordance with the systems notices as published in the periodic OPNAVNOTEs 5211, subj: CURRENT PA ISSUANCES.

(2) Maintain accountability records of disclosures (use enclosure (10) to account for all disclosure accountings outside DOD).

h. DON Employees. Each employee of the DON 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 instruction.

(2) Not maintaining unpublished official files which would fall under the provisions of reference (a).

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

7. Systems of Records. To be subject to this instruction, 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 DON.

a. Retrieval Practices

(1) Records in a group of records that are not retrieved by personal identifiers are not covered by this instruction, even if the records contain information about individuals and are

under the control of DON. 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 paragraph 9a.

(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 instruction and the records system notice should be deleted in accordance with paragraph 9d.

b. Recordkeeping Standards. A record maintained in a system of records subject to this instruction 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 and also must be related to a lawful purpose or mission of the DON activity maintaining the record.

(3) **Be timely.** All information in the record must be reviewed periodically to ensure that it has not changed due to time or later events.

(4) **Be complete.** It must be able to stand alone in accomplishing the purpose for which it is maintained.

(5) **Be necessary.** All information in the record must be needed to accomplish a DON mission or purpose established by Federal Law or E.O. of the President.

c. Authority to Establish Systems of Records. Identify the specific Federal statute or E.O. of the President that authorizes maintaining each system of records. When a naval activity

uses its "internal housekeeping" statute, i.e., 5 U.S.C. 301, Departmental Regulations, the naval instruction that implements the statute should also be identified. A statute or E.O. authorizing a system of records does not negate the responsibility to ensure the information in the system of records is relevant and necessary.

d. Exercise of First Amendment Rights

(1) Do not maintain any records describing how an individual exercises rights guaranteed by the First Amendment of the U.S. Constitution unless expressly authorized by Federal law; the individual; or 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.

e. System Manager's Evaluations and Reviews

(1) Evaluate each new system of records. Before establishing a system of records, evaluate the information to be included and consider the following:

(a) The relationship of each item of information to be collected and retained to the purpose for which the system is maintained (all information must be relevant to the purpose);

(b) The specific impact on the purpose or mission if each category of information is not collected (all information must be necessary to accomplish a lawful purpose or mission.);

(c) The ability to meet the informational needs without using personal identifiers (will anonymous statistical records meet the needs?);

(d) The length of time each item of information must be kept;

(e) The methods of disposal;

(f) The cost of maintaining the information; and

(g) Whether a system already exists that serves the purpose of the new system.

(2) Evaluate and review all existing systems of records.

(a) When an alteration or amendment of an existing system is prepared pursuant to paragraphs 9b and 9c, do the evaluation described in paragraph 7e.

(b) Conduct the following reviews annually and be prepared to report, in accordance with paragraph 6c(8), the results and corrective actions taken to resolve problems uncovered.

1. Training practices to ensure all personnel are familiar with the requirements of references (a) and (b), this instruction, and any special needs their specific jobs entail.

2. Recordkeeping and disposal practices to ensure compliance with this instruction.

3. Ongoing computer matching programs in which records from the system have been matched with non-DOD records to ensure that the requirements of paragraph 20 have been met.

4. Actions of DON personnel that resulted in either DON being found civilly liable or a person being found criminally liable under reference (a), to determine the extent of the problem and find the most effective way of preventing the problem from occurring in the future.

5. Each system of records notice to ensure it accurately describes the system. Where major changes are needed, alter the system notice in accordance with paragraph

9b. If minor changes are needed, amend the system notice pursuant to paragraph 9c.

(c) Every even-numbered year, review a random sample of DON contracts that provide for the operation of a system of records to accomplish a DON function, to ensure the wording of each contract complies with the provisions of reference (a) and paragraph 7h of this instruction.

(d) Every three years, beginning in 1992, review the routine use disclosures associated with each system of records to ensure the recipient's use of the records continues to be compatible with the purpose for which the information was originally collected.

(e) Every three years, beginning in 1993, review each system of records for which exemption rules have been established to determine whether each exemption is still needed.

(f) When directed, send the reports through proper channels to the CNO (OP-09B30).

f. Discontinued Information Requirements

(1) Immediately stop collecting any category or item of information about individuals that is no longer justified, and when feasible, remove the information from existing records.

(2) Do not destroy records that must be kept in accordance with retention and disposal requirements established under SECNAVINST 5212.5, Disposal of Navy and Marine Corps Records.

g. Review Records Before Disclosing Outside the Federal Government. Before disclosing a record from a system of records to anyone outside the Federal Government, take reasonable steps to ensure the record which is being disclosed is accurate, relevant, timely, and complete for the purposes it is being maintained.

h. Federal Government Contractors

(1) Applicability to Federal Government Contractors.

(a) When a naval activity contracts for the operation of a system of records to accomplish its function, the activity must ensure compliance with this instruction and reference (a). For the purposes of the criminal penalties described in reference (a), the contractor and its employees shall be considered employees of the agency during the performance of the contract.

(b) Consistent with Parts 24 and 52 of the Federal Acquisition Regulation (FAR), contracts for the operation of a system of records shall identify specifically the record system and the work to be performed, and shall include in the solicitations and resulting contract the terms as prescribed by the FAR.

(c) If the contractor must use records that are subject to this instruction to perform any part of a contract, the contractor activities are subject to this instruction.

(d) This instruction does not apply to records of a contractor that are:

1. Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

2. Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the naval activity;

3. Maintained as training records by an educational organization contracted by a naval activity to provide training when the records of the contract students are similar to and commingled with training records of other students, such as admission forms, transcripts, and academic counseling and similar records; or

4. Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with 31 U.S.C. § 952d.

(e) For contracting that is subject to this instruction, naval activities shall publish instructions that:

1. Furnish PA guidance to personnel who solicit, award, or administer Government contracts;

2. Inform prospective contractors of their responsibilities under this instruction and the DON Privacy Program;

3. Establish an internal system for reviewing contractor's performance for compliance with the PA; and

4. Provide for the biennial review of a random sample of contracts that are subject to this instruction.

(2) **Contracting Procedures.** The Defense Acquisition Regulatory (DAR) Council, which oversees the implementation of the FAR within DOD, is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts that are subject to this instruction and reference (a).

(3) **Contractor Compliance.** Naval activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council under the preceding subparagraph.

(4) **Disclosing Records to Contractors.** Disclosing records to a contractor for use in performing a contract let by a naval activity is considered a disclosure within DON. The contractor is considered the agent of DON when receiving and maintaining the records for that activity.

8. **Safeguarding Records in Systems of Records.** Establish appropriate administrative, technical, and physical safeguards to ensure the

records in every system of records are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

a. Minimum Standards

(1) Conduct risk analysis and management planning for each system of records. Consider sensitivity and use of the records, present and projected threats and vulnerabilities, and present and projected cost-effectiveness of safeguards. The risk analysis may vary from an informal review of a small, relatively insensitive system to a formal, fully quantified risk analysis of a large, complex, and highly sensitive system.

(2) Train all personnel operating a system of records or using records from a system of records in proper record security procedures.

(3) Label information exempt from disclosure under this instruction to reflect their sensitivity, such as "FOR OFFICIAL USE ONLY," "PRIVACY ACT SENSITIVE: DISCLOSE ON A NEED-TO-KNOW BASIS ONLY," or some other statement that alerts individuals of the sensitivity to the records.

(4) Administer special administrative, physical, and technical safeguards to protect records processed or stored in an automated data processing or word processing system to protect them from threats unique to those environments. Special considerations for using and safeguarding records in computerized systems of records is contained in enclosure (6). Special considerations for safeguarding records during word processing is contained in enclosure (7).

b. Records Disposal

(1) Dispose of records from systems of records so as to prevent inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (i.e., such as tearing, burning,

melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) The transfer of large volumes of records (e.g., printouts and computer cards) in bulk to a disposal activity such as a Defense Reutilization and Marketing Office for authorized disposal is not a disclosure of records, if the volume of records, coding of the information, or some other factor render it impossible to recognize any personal information about a specific individual.

(3) When disposing or destroying large quantities of records from a system of records, care must be taken to ensure that the bulk of the records is maintained to prevent easy identification of specific records. If such bulk is maintained, no special procedures are required. If bulk is not maintained, or if the form of the records makes individually identifiable information easily discernable, dispose of the records in accordance with paragraph 8b(1).

9. Criteria for Creating, Altering, Amending and Deleting PA Systems of Records

a. Criteria for a New System of Records.

A new system of records is one for which no existing system notice has been published in the Federal Register. If a notice for a system of records has been cancelled or deleted, and it is determined that it should be reinstated or reused, a new system notice must be published in the Federal Register. Advance public notice must 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.

Enclosure (2) contains an explanation of the data elements required for any system of records notice to be published in the Federal Register. Also at enclosure (2) is a sample Report on a New System of Records submission. It includes a sample Narrative Statement and a System of Records Notice.

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 DON.

(7) Retrieving by SSNs, records that previously 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. (See enclosure (3)).

c. Criteria for Amending a System of Records Notice. Minor changes to published system of records notices are considered amendments. All amendments should be forwarded to CNO (OP-09B30) 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 (see enclosure (4)).

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 instruction, 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 (see enclosure (5)).

10. 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 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/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 PA 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 DON, 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/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 Manual must be consulted when soliciting SSNs for use in systems of records maintained by the Office of Personnel Management.

(7) A DON 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 1 January 1975. However, the separate PAS for the SSN, alone, or a merged PAS 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/her SSN, the activity must be prepared to identify the individual by alternate means.

d. Contents of PAS

(1) When an individual is requested to furnish information about himself/herself for a system of records, a PAS must be provided to the individual, regardless of the method used to collect the information (i.e., forms, personal or telephonic interview, etc). Enclosure (8) contains a general purpose PAS form (OPNAV 5211/12) which can be tailored to the purpose for which information is being requested and used when the PAS is not attached to the form. If the information requested will not be included in a system of records, a PAS is not required.

(2) The PAS shall include the following:

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

(b) 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.);

(c) The principle purposes for collecting the information;

(d) The routine uses that will be made of the information (i.e., to whom and why it will be disclosed outside the DOD); and

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

(3) The PAS 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 PAS 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 PAS. Enclosure (8) also contains an actual form with the PAS included.

e. **Format for PAS.** When forms are used to collect information about individuals for a system of records, the PAS 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 PAS),

(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.

11. 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 instruction, 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 instruction.

(2) **Notification of Record's Existence.** Each naval activity shall establish procedures for notifying an individual, in response to his/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 access to records in systems of records to the system manager or the office designated in the DON compilation of system notices (periodic OPNAV-NOTES 5211, subj: CURRENT PA ISSUANCES).

(4) Verifying Identity

(a) An individual shall provide reasonable verification of identity before obtaining access to records.

(b) 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."

(c) 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).

(d) 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.

(e) Allow an individual to be accompanied by a person of his/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.

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

(g) Do not require the individual to explain why he/she is seeking access to a record under this instruction.

(h) Only a designated denial authority may deny access. The denial must be in writing and contain the information required by paragraph 11d of this instruction.

(5) **Blanket Requests not Honored.** Do not honor requests from individuals for notification and/or access concerning all DON systems of records. In these instances, notify the

individual that requests for notification and/or access must be directed to the appropriate system manager for the particular record system being requested, as indicated in the periodic OPNAV-NOTES 5211, subj: CURRENT PA ISSU-ANCES; and the request must either designate the particular system of records to be searched, or provide sufficient information for the system manager to identify the appropriate system. Also, provide the individual with any other information needed for obtaining consideration of his/her request.

(6) Granting Individual Access to Records

(a) Grant the individual access to the original record (or exact copy) without any changes or deletions, other than those made in accordance with paragraph (15).

(b) Grant the individual's request for an exact copy of the record, upon the signed authorization of the individual, and provide a copy to anyone designated by the individual. In either case, the copying fees may be assessed to the individual pursuant to paragraph 11b.

(c) If requested, explain any record or portion of a record that is not understood, as well as any changes or deletions.

(7) Illegible or Incomplete Records. Do not deny an individual access solely because the physical condition or format of the record does not make it readily available (i.e., when the record is in a deteriorated state or on magnetic tape). Either prepare an extract or recopy the document exactly.

(8) Access by Parents and Legal Guardians

(a) The parent of any minor, or the legal guardian of any individual declared by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age, may obtain access to the record of the minor or incompetent individual if the parent or legal

guardian is acting on behalf or for the benefit of the minor or incompetent. However, with respect to access by parents and legal guardians to medical records and medical determinations about minors, use the following procedures:

1. In the United States, the laws of the state where the records are located might afford special protection to certain medical records (i.e., drug and alcohol abuse treatment, and psychiatric records). The state statutes might apply even if the records are maintained by a naval medical facility.

2. For installations located outside the U.S., the parent or legal guardian of a minor shall be denied access if all four of the following conditions are met:

a. The minor at the time of the treatment or consultation was 15, 16, or 17 years old;

b. The treatment or consultation was within a program authorized by law or regulation to provide confidentiality to the minor;

c. The minor indicated a desire that the treatment or consultation record be handled in confidence and not disclosed to a parent or guardian; and

d. The parent or legal guardian does not have the written authorization of the minor or a valid court order granting access.

(b) A minor or incompetent has the same right of access as any other individual under this instruction. The right of access of the parent or legal guardian is in addition to that of the minor or incompetent.

(9) Access to Information Compiled in Reasonable Anticipation of A Civil Proceeding

(a) An individual is not entitled under this instruction to access information compiled in reasonable anticipation of a civil action or proceeding.

(b) The term "civil action or proceeding" includes quasi-judicial and pre-trial judicial proceedings, as well as formal litigation.

(c) Paragraphs 11a(9)(a) and (b), do not prohibit access to records compiled or used for purposes other than litigation, nor prohibit access to systems of records solely because they are frequently subject to litigation. The information must have been compiled for the primary purpose of litigation.

(10) Personal Notes or Records not under the Control of the DON

(a) Certain documents under the control of a DON employee and used to assist him/her in performing official functions are not considered DON records within the meaning of this instruction. These documents are not systems of records that are subject to this instruction, if they are:

1. Maintained and discarded solely at the discretion of the author;
2. Created only for the author's personal convenience;
3. Not the result of official direction or encouragement, whether oral or written; and
4. Not shown to other persons for any reason or filed in agency files.

(11) Relationship between the PA and FOIA. In some instances, individuals requesting access to records pertaining to themselves may not know which Act to cite as the appropriate statutory authority. The following guidelines are to ensure that the individuals receive the greatest degree of access under both Acts:

(a) Access requests that specifically state or reasonably imply that they are made under reference (d), are processed under reference (e).

(b) Access requests that specifically state or reasonably imply that they are made under reference (a) are processed under this instruction.

(c) Access requests that cite both references (a) and (e) are processed under the Act that provides the greater degree of access. Inform the requester which instruction was used in granting or denying access.

(d) Do not penalize the individual access to his/her records otherwise releasable under reference (a) and periodic OPNAVNOTES 5211, subj: CURRENT PA ISSUANCES, simply because he/she failed to cite the appropriate statute or instruction.

(12) Time Limits. Acknowledge requests for access made under PA or this instruction within 10 working days after receipt, and advise the requester of your decision to grant/deny access within 30 working days.

b. Reproduction Fees. Normally, only one copy of any record or document will be provided. Checks or money orders for fees should be made payable to the Treasurer of the United States and deposited to the miscellaneous receipts of the treasury account maintained at the finance office servicing the activity.

(1) Fee schedules shall include only the direct cost of reproduction and shall not include costs of: (a) time or effort devoted to searching for or reviewing the record by naval personnel; (b) fees not associated with the actual cost of reproduction; (c) producing a copy when it must be provided to the individual without cost under another regulation, directive, or law; (d) normal postage; (e) transportation of records or personnel; or (f) producing a copy when the individual has requested only to review the record and has not requested a copy to keep, and the only means of allowing review is to make a copy (e.g., the record is stored in a computer and a copy must be printed to provide individual access, or the naval activity does not

wish to surrender temporarily the original record for the individual to review).

(2) Fee schedules.

(a) Office copy (per page) . . \$.10

(b) Microfiche (per fiche) . . \$.25

(3) Fee waivers. Waive fees automatically if the direct cost of reproduction is less than \$15, unless the individual is seeking an obvious extension or duplication of a previous request for which he/she was granted a waiver. Decisions to waive or reduce fees that exceed \$15 are made on a case-by-case basis.

c. Denying Individual Access

(1) Deny the record subject access to requested record only if it was compiled in reasonable anticipation of a civil action or proceeding (see paragraph 11a(9)) or is in a system of records that has been exempt from the access provisions of this instruction (see paragraph 15).

(2) Deny the individual access only to those portions of the record for which the denial will serve a legitimate government purpose. An individual may be refused access for failure to comply with established procedural requirements, but must be told the specific reason for the refusal and the proper access procedures.

(3) Deny the individual access to his/her medical and psychological records if it is determined that access could have an adverse affect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical practitioner. If it is medically indicated that access could have an adverse mental or physical effect on the individual, provide the record to a medical practitioner named by the individual, along with an explanation of why access without medical supervision could be harmful to the individual. In any case, do not require the named medical practitioner to request the record for the individual. If, however, the individual refuses or fails to designate a medical practitioner, access

shall be refused. The refusal is not considered a denial for reporting purposes under the PA.

d. Notifying the Individual. Written denial of access must be given to the individual. The denial letter shall include: (1) The name, title, and signature of a designated denial authority; (2) the date of the denial; (3) the specific reason for the denial, citing the appropriate subsections of reference (a) or this instruction authorizing the denial; (4) the individual's right to appeal the denial within 60 calendar days of the date the notice is mailed; and (5) the title and address of the review authority.

12. Amendment of Records

a. Individual Review and Amendment.

Encourage individuals to review periodically, the information maintained about them in systems of records, and to avail themselves of the amendment procedures established by this instruction.

(1) Right to Amend. An individual may request to amend any record retrieved by his/her personal identifier from a system of records, unless the system has been exempt from the amendment procedures under paragraph 12 of this instruction. Amendments under this instruction are limited to correcting factual matters, not matters of opinion (i.e., information contained in evaluations of promotion potential or performance appraisals). When records sought to be amended are covered by another issuance, the administrative procedures under that issuance must be exhausted before using the PA. In other words, the PA may not be used to avoid the administrative procedures required by the issuance actually covering the records in question.

(2) In Writing. Amendment requests shall be in writing, except for routine administrative changes, such as change of address.

(3) Content of Amendment Request. An amendment request must include a description of the information to be amended; the reason for the amendment; the type of amendment

action sought (i.e., deletion, correction, or addition); and copies of available documentary evidence supporting the request.

b. Burden of Proof. The individual must provide adequate support for the request.

c. Verifying Identity. The individual may be required to provide identification to prevent the inadvertent or intentional amendment of another's record. Use the verification guidelines provided in paragraph 11a(4) of this instruction.

d. Limits on Amending Judicial and Quasi-Judicial Evidence and Findings. This instruction does not permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Amendments to such records must be made in accordance with procedures established for such proceedings. This instruction does not permit a collateral attack on a judicial or quasi-judicial finding; however, this instruction may be used to challenge the accuracy of recording the finding in a system of records.

e. Standards for Amendment Request Determinations. The record which the individual requests to be amended must meet the recordkeeping standards established in paragraph 7b. The record must be accurate, relevant, timely, complete, and necessary. If the record in its present state does not meet each of the criteria, grant the amendment request to the extent necessary to meet them.

f. Time Limits. Within 10 working days of receiving an amendment request, the systems manager shall provide the individual a written acknowledgement of the request. If action on the amendment request is completed within the 10 working days and the individual is so informed, no separate acknowledgment is necessary. The acknowledgment must clearly identify the request and advise the individual when to expect notification of the completed action. Only under exceptional circumstances should more than 30 working days be required to complete the action on an amendment request.

g. Granting an Amendment Request in Whole or in Part

(1) Notify the Requester. To the extent the amendment request is granted, the systems manager shall notify the individual and make the appropriate amendment.

(2) Notify Previous Recipients. Notify all previous recipients of the information (as reflected in the disclosure accounting record) that the amendment has been made and provide each a copy of the amended record. Recipients who are known to be no longer retaining the record need not be advised of the amendment. If it is known that other naval activities, DOD components, or Federal agencies have been provided the information that now requires amendment, or if the individual requests that these agencies be notified, provide the notification of amendment even if those activities or agencies are not listed on the disclosure accounting form.

h. Denying an Amendment Request in Whole or in Part. If the amendment request is denied in whole or in part, promptly notify the individual in writing. Include in the notification to the individual the following:

(1) Those sections of reference (a) or this instruction upon which the denial is based; (2) his/her right to appeal to the head of the activity for an independent review of the initial denial; (3) the procedures for requesting an appeal, including the title and address of the official to whom the appeal should be sent; and (4) where the individual can receive assistance in filing the appeal.

i. Requests for Amending OPM Records. The records in an OPM government-wide system of records are only temporarily in the custody of naval activities. Requests for amendment of these records must be processed in accordance with reference (f). The denial authority may deny a request, but all denials are subject to review by the Assistant Director for Workforce

Information, Personnel Systems Oversight Group, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415.

j. Individual's Statement of Disagreement

(1) If the review authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement listing the reasons for disagreeing with the refusal to amend.

(2) If possible, incorporate the statement of disagreement into the record. If that is not possible, annotate the record to reflect that the statement was filed and maintain the statement so that it can be readily obtained when the disputed information is used or disclosed.

(3) Furnish copies of the statement of disagreement to all individuals listed on the disclosure accounting form (except those known to be no longer retaining the record), as well as to all other known holders of copies of the record.

(4) Whenever the disputed information is disclosed for any purpose, ensure that the statement of disagreement also is used or disclosed.

k. DON Statement of Reasons

(1) If the individual files a statement of disagreement, the naval activity may file a statement of reasons containing a concise summary of the activity's reasons for denying the amendment request.

(2) The statement of reasons shall contain only those reasons given to the individual by the appellate official and shall not contain any comments on the individual's statement of disagreement.

(3) At the discretion of the naval activity, the statement of reasons may be disclosed to those individuals, activities, and agencies that receive the statement of disagreement.

13. PA Appeals

a. How to File an Appeal. The following guidelines shall be followed by individuals wishing to appeal a denial of notification, access, or amendment of records.

(1) The appeal must be received by the cognizant review authority (i.e., ASN (M&RA), NJAG, OGC, or OPM) within 60 calendar days of the date of the response.

(2) The appeal must be in writing and requesters should provide a copy of the denial letter and a statement of their reasons for seeking review.

b. Time of Receipt. The time limits for responding to an appeal commence when the appeal reaches the office of the review authority having jurisdiction over the record. Misdirected appeals should be referred expeditiously to the proper review authority.

c. Review Authorities. ASN (M&RA), NJAG, and OGC are authorized to adjudicate appeals made to SECNAV. NJAG and OGC are further authorized to delegate this authority to a designated Assistant NJAG and the Principal Deputy General or Deputy General Counsel, respectively, under such terms and conditions as they deem appropriate.

(1) If the record is from a civilian Official Personnel Folder or is contained on any other OPM forms, send the appeal to the Assistant Director for Workforce Information, Personnel Systems and Oversight Group, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415. Records in all systems of records maintained in accordance with the OPM government-wide systems notices are only in the temporary custody of the DON.

(2) If the record pertains to the employment of a present or former Navy and Marine Corps civilian employee, such as Navy or Marine

Corps civilian personnel records or an employee's grievance or appeal file, to the General Counsel, Navy Department, Washington, DC 20360-5110.

(3) If the record pertains to a present or former military member's fitness reports or performance evaluations to the Assistant Secretary of the Navy (Manpower and Reserve Affairs), Navy Department, Washington, DC 20350-1000.

(4) All other records dealing with present or former military members to the Judge Advocate General, Navy Department, 200 Stovall Street, Alexandria, VA 22332-2400.

d. Appeal Procedures

(1) If the appeal is granted, the review authority shall advise the individual that his/her appeal has been granted and provide access to the record being sought.

(2) If the appeal is denied totally or in part, the appellate authority shall advise the reason(s) for denying the appeal, citing the appropriate subsections of reference (a) or this instruction that apply; the date of the appeal determination; the name, title, and signature of the appellate authority; and a statement informing the requester of his/her right to seek judicial relief in the Federal District Court.

e. Final Action, Time Limits and Documentation

(1) The written appeal notification granting or denying access is the final naval activity action on the initial request for access.

(2) All appeals shall be processed within 30 working days of receipt, unless the appellate authority finds that an adequate review cannot be completed within that period. If additional time is needed, notify the applicant in writing, explaining the reason for the delay and when the appeal will be completed.

f. Denial of Appeal by Activity's Failure to Act. An individual may consider his/her appeal denied if the appellate authority fails to:

(1) Take final action on the appeal within 30 working days of receipt when no extension of time notice was given; or

(2) Take final action within the period established by the notice to the appellate authority of the need for an extension of time to complete action on the appeal.

14. Disclosure of Records

a. Conditions of Disclosure

(1) Reference (a) prohibits an agency from disclosing any record contained in a system of records to any person or agency, except when the record subject gives written consent for the disclosure or when one of the 12 conditions listed below in paragraph 14b applies.

(2) Except for disclosures made under references (d) and (e), before disclosing any record from a system of records to any recipient other than a Federal agency, make reasonable efforts to ensure the record is accurate, relevant, timely, and complete for DON purposes. Records discovered to have been improperly filed in the system of records should be removed before disclosure.

(a) If validation cannot be obtained from the record itself, the naval activity may contact the record subject (if reasonably available) to verify the accuracy, timeliness, completeness, and relevancy of the information.

(b) If validation cannot be obtained from the record and the record subject is not reasonably available, advise the recipient that the information is believed to be valid as of a specific date and reveal any factors bearing on the validity of the information.

b. Nonconsensual Disclosures. Reference (a) provides 12 instances when a record in a system of records may be disclosed without the written consent of the record subject:

(1) Disclosures within DOD. For purposes of disclosing records, the Department of Defense is considered a single agency; hence, a record may be disclosed to any officer or employee in the DOD (including private contractor personnel who are engaged to perform services needed in connection with the operation of a system of records for a DOD component), who have a need for the record in the performance of their duties, provided this use is compatible with the purpose for which the record is maintained. This provision is based on the "need to know" concept.

(a) For example, this may include disclosure to personnel managers, review boards, discipline officers, courts-martial personnel, medical officers, investigating officers, and representatives of the Judge Advocate General, Auditor General, Naval Inspector General, or the Naval Investigative Service, who require the information in order to discharge their official duties. Examples of personnel outside the DON who may be included are: personnel of the Joint Staff, Armed Forces Entrance and Examining Stations, Defense Investigative Service, or the other military departments, who require the information in order to discharge an official duty.

(b) It may also include the transfer of records between naval components and non-DOD agencies in connection with the Personnel Exchange Program (PEP) and interagency support agreements. Disclosure accountings are not required for intra-agency disclosure and disclosures made in connection with interagency support agreements or the PEP. Although some disclosures authorized by this subparagraph might also meet the criteria for disclosure under other exceptions specified in the following subparagraphs, they should be treated under this subparagraph for disclosure accounting purposes.

(2) Disclosures Required by the FOIA

(a) A record must be disclosed if required by reference (d), which is implemented by reference (e).

(b) References (d) and (e) require that records be made available to any person requesting them in writing, unless the record is exempt from disclosure under one of the nine FOIA exemptions. Therefore, if a record is not exempt from disclosure, it must be provided to the requester.

(c) Certain records, such as personnel, medical, and similar files, are exempt from disclosure under exemption (b)(6) of reference (d). Under that exemption, disclosure of information pertaining to an individual can be denied only when the disclosure would be a clearly unwarranted invasion of personal privacy. The first step is to determine whether a viable personal privacy interest exists in these records involving an identifiable living person. The second step is to consider how disclosure would benefit the general public in light of the content and context of the information in question. The third step is to determine whether the identified public interests qualify for consideration. The fourth step is to balance the personal privacy interests against the qualifying public interest. Numerous factors must be considered such as: the nature of the information to be disclosed (i.e., Do individuals normally have an expectation of privacy in the type of information to be disclosed?); importance of the public interest served by the disclosure and probability of further disclosure which may result in an unwarranted invasion of privacy; relationship of the requester to the public interest being served; newsworthiness of the individual to whom the information pertains (i.e., high ranking officer, public figure); degree of sensitivity of the information from the standpoint of the individual or the individual's family, and its potential for being misused to the harm, embarrassment, or inconvenience of the individual or the individual's family; the passage of time since the event which is the topic of the record (i.e., to disclose

that an individual has been arrested and is being held for trial by court-martial is normally permitted, while to disclose an arrest which did not result in conviction might not be permitted after the passage of time); and the degree to which the information is already in the public domain or is already known by the particular requester.

(d) Records or information from investigatory records, including personnel security investigatory records, are exempt from disclosure under the broader standard of "an unwarranted invasion of personal privacy" found in exemption (b)(7)(C) of reference (d). This broader standard applies only to records or information compiled for law enforcement purposes.

R) (e) A disclosure under reference (d) about military members must be in accordance with reference (e), but the following information normally may be disclosed from military personnel records (except for those personnel assigned to sensitive, routinely deployable units or stationed in foreign territories), without a clearly unwarranted invasion of personal privacy: full name, rank, date of rank, base pay, past duty stations, present duty station and future duty station (if finalized), unless the stations have been determined by the DON to be sensitive, routinely deployable, or located in a foreign territory (see paragraph 9p of reference (e)), office or duty telephone number, source of commission, promotion sequence number, awards and decorations, attendance at professional military schools, and duty status at any given time.

(f) The following information normally may be disclosed from civilian employee records about CONUS employees: full name, present and past position titles and occupational series, present and past grades, present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious and Distinguished Executive Ranks, and allowances and differentials), past duty stations, present duty station and future duty station (if finalized), including room numbers, shop designations, or other identifying information regarding buildings or places of employment, unless the duty stations have been

determined by the DON to be sensitive, routinely deployable, or located in a foreign territory, position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) that the disclosure of which would not interfere with law enforcement programs or severely inhibit DON effectiveness.

(g) Disclosure of home addresses and home telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, they may be disclosed if the individual has consented to the disclosure; the disclosure is required by the FOIA; the disclosure is required by another law, such as 42 U.S.C. 653 (reference (g)), which provides assistance to states in locating parents who have defaulted on child support payments, or the collection of alimony, and to state and local tax authorities for the purpose of enforcing tax laws. However, care must be taken prior to release to ensure that a written record is prepared to document the reasons for the release determination.

1. When compiling home addresses and telephone numbers, the individual may be offered the option of authorizing disclosure of the information without further consent for specific purposes, such as locator services. In that case, the information may be disclosed for the stated purpose without further consent. If the information is to be disclosed for any other purpose, a signed consent permitting the additional disclosure must be obtained from the individual.

2. Before listing home addresses and telephone numbers in DON telephone directories, give the individual the opportunity to refuse such a listing. If the individual requests that the home address or telephone number not be listed in the directory, do not assess any additional fee associated with maintaining an unlisted number for government-owned telephone services.

3. The sale or rental of lists of names and addresses is prohibited unless such action is specifically authorized by Federal law.

This does not prohibit the disclosure of names and addresses made under reference (e).

4. In response to FOIA requests, information concerning special and general courts-martial results (e.g., records of trial) are releasable. However, information regarding summary courts-martial and non-judicial punishment are generally not releasable. The balancing of interests must be done. It is possible that in a particular case, information regarding non-judicial punishment should be disclosed pursuant to a FOIA request (i.e., the facts leading to a nonjudicial punishment are particularly newsworthy or the case involves a senior official abusing the public trust through office-related misconduct, such as embezzlement). Announcement of nonjudicial punishment dispositions under JAGMAN, subsection 0107, is a proper exercise of command authority and not a release of information under FOIA or this instruction. Exceptions to this policy must be coordinated with CNO (OP-09B30) or CMC (MI-3) prior to responding to requesters, including all requests for this type of information from members of Congress.

(3) Disclosures for Established Routine Uses

(a) Records may be disclosed outside DON if the disclosure is for an established routine use.

(b) A routine use shall:

1. Be compatible with and related to the purpose for which the record was created;

2. Identify the persons or organizations to whom the record may be disclosed;

3. Identify specifically the uses for which the information may be employed by the receiving person or organization; and

4. Have been published previously in the Federal Register.

(c) A routine use shall be established for each user of the information outside the DON who needs the information for an official purpose.

(d) Routine uses may be established, discontinued, or amended without the consent of the individuals to whom the records pertain. However, new and amended routine uses must be published in the Federal Register at least 30 days before the information may be disclosed under their provisions.

(e) In addition to the routine uses established by the DON for each system of records, common "Blanket Routine Uses," applicable to all record systems maintained with the DON, have been established. These "Blanket Routine Uses" are published at the beginning of the DON's Federal Register compilation of record systems notices rather than at each system notice and are also reflected in periodic OPNAVNOTEs 5211, subj: CURRENT PA ISSUANCES. A copy of the "Blanket Routine Uses" are at enclosure (9). Unless a system notice specifically excludes a system of records from a "Blanket Routine Use," all "Blanket Routine Uses" apply to that system.

(f) If the recipient has not been identified in the F.R. or if the recipient, though identified, intends to employ the information for a purpose not published in the Federal Register, the written consent of the individual is required before the disclosure can be made.

(4) Disclosures to the Bureau of the Census. Records may be disclosed to the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activities authorized by 13 U.S.C. § 8.

(5) Disclosures for Statistical Research or Reporting. Records may be disclosed to a recipient for statistical research or reporting if:

(a) Prior to the disclosure, the recipient has provided adequate written assurance that the records shall be used solely for statistical research or reporting; and

(b) The records are transferred in a form that does not identify individuals.

(6) Disclosures to the National Archives and Records Administration

(a) Records may be disclosed to the National Archives and Record Administration for evaluation to determine whether the records have sufficient historical or other value to warrant preservation by the Federal government. If preservation is warranted, the records will be retained by the National Archives and Record Administration, which becomes the official owner of the records.

(b) Records may be disclosed to the National Archives and Record Administration to carry out records management inspections required by Federal law.

(c) Records transferred to a Federal Records Center operated by the National Archives and Record Administration for storage are not within this category. Those records continue to be maintained and controlled by the transferring naval activity. The Federal Records Center is considered the agent of DON and the disclosure is made under paragraph 14b(1) of this instruction.

(7) Disclosures When Requested for Law Enforcement Purposes

(a) A record may be disclosed to another agency or an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if:

1. The civil or criminal law enforcement activity is authorized by law (federal, state or local); and

2. The head of the agency (or his/her designee) has made a written request to the naval activity specifying the particular record or portion desired and the law enforcement purpose for which it is sought.

(b) Blanket requests for any and all records pertaining to an individual shall not be honored. The requesting agency must specify each record or portion desired and how each relates to the authorized law enforcement activity.

(c) If a naval activity discloses a record outside the DOD for law enforcement purposes without the individual's consent and without an adequate written request, the disclosure must be under an established routine use, such as the "Blanket Routine Use" for law enforcement.

(d) Disclosure to foreign law enforcement agencies is not governed by the provisions of reference (a) and this paragraph, but may be made only under established in "Blanket Routine Uses," routine uses published the individual record system notice, or to other governing authority.

(8) Disclosure to Protect the Health or Safety of an Individual. Disclosure may be made under emergency conditions involving circumstances affecting the health and safety of an individual (i.e., when the time required to obtain the consent of the individual to whom the records pertain might result in a delay which could impair the health or safety of a person) provided notification of the disclosure is sent to the record subject. Sending the notification to the last known address is sufficient. In instances where information is requested by telephone, an attempt will be made to verify the inquirer's and medical facility's identities and the caller's telephone number. The requested information, if then considered appropriate and of an emergency nature, may be provided by return call.

(9) Disclosures to Congress

(a) A record may be disclosed to either House of Congress at the request of either the Senate or House of Representatives as a whole.

(b) A record also may be disclosed to any committee, subcommittee, or joint committee of Congress if the disclosure pertains to a matter within the legislative or investigative jurisdiction of the committee, subcommittee, or joint committee.

(c) Disclosure may not be made to a Member of Congress requesting in his/her individual capacity. However, for Members of Congress making inquiries on behalf of individuals who are subjects of records, a "Blanket Routine Use" has been established to permit disclosures to individual Members of Congress.

1. When responding to a congressional inquiry made on behalf of a constituent by whose identifier the record is retrieved, there is no need to verify that the individual has authorized the disclosure to the Member of Congress.

2. The oral or written statement of a Congressional staff member is sufficient to establish that a request has been received from the individual to whom the record pertains.

3. If the constituent inquiry is made on behalf of an individual other than the record subject, provide the Member of Congress only that information releasable under reference (d). Advise the Member of Congress that the written consent of the record subject is required before additional information may be disclosed. Do not contact the record subject to obtain consent for the disclosure to the Member of Congress unless the Congressional office specifically requests it be done.

(10) Disclosures to the Comptroller General for the General Accounting Office (GAO). Records may be disclosed to the

Comptroller General of the U.S., or authorized representative, in the course of the performance of the duties of the GAO.

(11) Disclosures under Court Orders

(a) Records may be disclosed under the order of a court of competent jurisdiction.

(b) When a record is disclosed under this provision and the compulsory legal process becomes a matter of public record, make reasonable efforts to notify the individual to whom the record pertains. Notification sent to the last known address of the individual is sufficient. If the order has not yet become a matter of public record, seek to be advised as to when it will become public. Neither the identity or the party to whom the disclosure was made nor the purpose of the disclosure shall be made available to the record subject unless the court order has become a matter of public record.

(c) The court order must bear the signature of a federal, state, or local judge. Orders signed by court clerks or attorneys are not deemed to be orders of a court of competent jurisdiction. A photocopy of the order, regular on its face, will be sufficient evidence of the court's exercise of its authority of the minimal requirements of SECNAVINST 5820.8A, "Release of Official Information for Litigation Purposes and Testimony by DON Personnel."

(12) Disclosures to Consumer

Reporting Agencies. Certain information may be disclosed to consumer reporting agencies (i.e., credit reference companies such as TRW and Equifax, etc.) as defined by the Federal Claims Collection Act of 1966 (31 U.S.C. § 952d). Under the provisions of that Act, the following information may be disclosed to a consumer reporting agency: (a) Name, address, taxpayer identification number (SSN), and other information necessary to establish the identity of the individual; (b) the amount, status, and history of the claim; and (c) the agency or program under which the claim arose.

31 U.S.C. § 952d specifically requires that the Federal Register notice for the system of records from which the information will be disclosed indicate that the information may be disclosed to a consumer reporting agency.

c. Disclosures to Commercial Enterprises. Records may be disclosed to commercial enterprises only under the criteria established by references (e) and (g).

(1) Any information required to be disclosed by references (e) and (g) may be disclosed to a requesting commercial enterprise (see paragraph 14c).

(2) Commercial enterprises may present a consent statement signed by the individual indicating specific conditions for disclosing information from a record. Statements such as the following, if signed by the individual, are considered sufficient to authorize the disclosure: I hereby authorize the Department of the Navy to verify my SSN or other identifying information and to disclose my home address and telephone number to authorized representatives of (name of commercial enterprise) to be used in connection with my commercial dealings with that enterprise. All information furnished will be used in connection with my financial relationship with (name of commercial enterprise).

(3) When a consent statement as described in the preceding subsection is presented, provide the information to the commercial enterprise, unless the disclosure is prohibited by another regulation or Federal law.

(4) Blanket consent statements that do not identify the DOD or DON, or that do not specify exactly the information to be disclosed, may be honored if it is clear that the individual, in signing the consent statement, was seeking a personal benefit (i.e., loan for a house or automobile) and was aware of the type of information necessary to obtain the benefit sought.

(5) Do not honor requests from commercial enterprises for official evaluations of

personal characteristics such as personal financial habits.

d. Disclosure of Health Care Records to the Public. This paragraph applies to disclosure of information to the news media and the public concerning individuals treated or hospitalized in DON medical facilities and, when the cost of care is paid by the DON, in non-Federal facilities.

(1) Disclosures without the individual's consent. Normally, the following information may be disclosed without the individual's consent:

(a) Information required to be released by references (e) and (g), as well as the information listed in paragraph 14b(2)(e) for military personnel and in paragraph 14b(2)(f) for civilian employees; and

(b) General information concerning medical conditions, i.e., date of admission or disposition; present medical assessment of the individual's condition if the medical practitioner has volunteered the information, i.e., the individual's condition presently is (stable) (good) (fair) (serious) (critical), and the patient is (conscious) (semi-conscious) (unconscious).

(2) Disclosures with the individual's consent. With the individual's informed consent, any information about the individual may be disclosed. If the individual is a minor or has been declared incompetent by a court of competent jurisdiction, the parent of the minor or appointed legal guardian of the incompetent may give consent on behalf of the individual.

e. Disclosure of Personal Information on Group/Bulk Orders. Do not use personal information including complete SSNs, home addresses and phone numbers, dates of birth, etc., on group/bulk orders. This personal information should not be posted on lists that everyone listed on the orders sees. Such a disclosure of personal information violates the PA and this instruction.

f. Disclosure Accounting. Keep an accurate record of all disclosures made from a record (including those made with the consent of the individual) except those made to DOD personnel for use in performing their official duties; and those made under the FOIA. Disclosure accounting is to permit the individual to determine what agencies or persons have been provided information from the record, enable DON activities to advise prior recipients of the record of any subsequent amendments or statements of dispute concerning the record, and provide an audit trail of DON's compliance with reference (a).

(1) Disclosure accountings shall contain the date of the disclosure; a description of the information disclosed; the purpose of the disclosure; and the name and address of the person or agency to whom the disclosure was made. Enclosure (10) contains the DON Disclosure Accounting form (OPNAV 5211/9).

(2) The record subject has the right of access to the disclosure accounting except when the disclosure was made at the request of a civil or criminal law enforcement agency under paragraph 14b(7); or when the system of records has been exempted from the requirement to provide access to the disclosure accounting.

g. Methods of Disclosure Accounting. Since the characteristics of various records maintained within the DON vary widely, no uniform method for keeping disclosure accountings is prescribed. The primary criteria are that the selected method be one which will:

(1) enable an individual to ascertain what persons or agencies have received disclosures pertaining to him/her;

(2) provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record; and

(3) provide a means to prove, if necessary that the activity has complied with the requirements of reference (a) and this instruction.

h. Retention of Disclosure Accounting. Maintain a disclosure accounting of the life of the record to which the disclosure pertains, or 5 years after the date of the disclosure, whichever is longer. Disclosure accounting records are normally maintained with the record, as this will ensure compliance with paragraph 14f(1).

15. Exemptions

a. Using Exemptions. No system of records is automatically exempt from all provisions of reference (a). A system of records is exempt from only those provisions of reference (a) that are identified specifically in the exemption rule for the system. Enclosure (11) contains the systems designated as exempt, the types of exemptions claimed, the authority and reasons for invoking the exemptions and the provisions of reference (a) from which each system has been exempt. Exemptions are discretionary on the part of DON and are not effective until published as a final rule in the Federal Register. The naval activity maintaining the system of records shall make a determination that the system is one for which an exemption may be established and then propose an exemption rule for the system. Submit the proposal to CNO (OP-09B30) for approval and publication in the Federal Register. A sample exemption rule proposal is at enclosure (12). To establish an exemption rule, refer to paragraph 15c.

b. Types of Exemptions. There are two types of exemptions permitted by reference (a).

(1) **General Exemptions.** Those that authorize the exemption of a system of records from all but specifically identified provisions of reference (a).

(2) **Specific Exemptions.** Those that allow a system of records to be exempt from only a few designated provisions of reference (a).

Enclosure (13) provides a quick and easy reference to assist in determining when a general or specific exemption may be claimed under the PA.

c. Establishing Exemptions

(1) Reference (a) authorizes SECNAV to adopt rules designating eligible systems of records as exempt from certain requirements. SECNAV has delegated the CNO (OP-09B30) to make a determination that the system is one for which an exemption may be established and then propose and establish an exemption rule for the system. No system of records within DON shall be considered exempt until the CNO (OP-09B30) has approved the exemption and an exemption rule has been published as a final rule in the Federal Register. A system of records is exempt from only those provisions or reference (a) that are identified specifically in the DON exemption rule for the system.

(2) No exemption may be established for a system of records until the system itself has been established by publishing a notice in the Federal Register, at least 30 days prior to the effective date, describing the system. This allows interested persons an opportunity to comment. An exemption may not be used to deny an individual access to information that he/she can obtain under reference (e).

d. Exemption for Classified Material.

All systems of records maintained by the DON shall be exempt under section (k)(1) of reference (a), to the extent that the systems contains any information properly classified under E.O. 12356 and that is required by that Executive Order to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information. NOTE: DON PA systems of records which contain classified information automatically qualify for a (k)(1) exemption, without establishing an exemption rule.

e. Exempt Records in Nonexempt Systems

(1) An exemption rule applies to the system of records for which it was established.

If a record from an exempt system is incorporated intentionally into a system that has not been exempt, the published notice and rules for the nonexempt system will apply to the record and it will not be exempt from any provisions of reference (a).

(2) A record from one component's (i.e., DON) exempted system that is temporarily in the possession of another component (i.e., Army) remains subject to the published system notice and rules of the originating component's (i.e., DON). However, if the non-originating component incorporates the record into its own system of records, the published notice and rules for the system into which it is incorporated shall apply. If that system of records has not been exempted, the record shall not be exempt from any provisions of reference (a).

(3) A record accidentally misfiled into a system of records is governed by the published notice and rules for the system of records in which it actually should have been filed.

f. General Exemptions

(1) Central Intelligence Agency (CIA).

The DON is not authorized to establish an exemption for records maintained by the CIA under subsection (j)(1) of reference (a).

(2) Law Enforcement

(a) The general exemption provided by subsection (j)(2) of reference (a) may be established to protect criminal law enforcement records maintained by DON.

(b) To be eligible for the (j)(2) exemption, the system of records must be maintained by an element that performs, as one of its principal functions, the enforcement of criminal laws. The Naval Investigative Service, Naval Inspector General, and military police activities qualify for this exemption.

(c) Criminal law enforcement includes police efforts to detect, prevent, control,

or reduce crime, or to apprehend criminals, and the activities of prosecution, court, correctional, probation, pardon, or parole authorities.

(d) Information that may be protected under the (j)(2) exemption includes:

1. Information compiled for the purpose of identifying criminal offenders and alleged criminal offenders consisting of only identifying data and notations of arrests; the nature and disposition of criminal charges; and sentencing, confinement, release, parole, and probation status;

2. Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; and

3. Reports identifiable to an individual, compiled at any stage of the enforcement process, from arrest, apprehension, indictment, or preferral of charges through final release from the supervision that resulted from the commission of a crime.

(e) The (j)(2) exemption does not apply to:

1. Investigative records maintained by a naval activity having no criminal law enforcement duties as one of its principle functions, or

2. Investigative records compiled by any element concerning individual's suitability, eligibility, or qualification for duty, employment, or access to classified information, regardless of the principle functions of the naval activity that compiled them.

(f) The (j)(2) exemption established for a system of records maintained by a criminal law enforcement activity cannot protect law enforcement records incorporated into a nonexempt system of records or any system of records maintained by an activity not principally tasked with enforcing criminal laws. All system managers, therefore, are cautioned to comply

strictly with DON regulations or instructions prohibiting or limiting the incorporation of criminal law enforcement records into systems other than those maintained by criminal law enforcement activities.

g. Specific Exemptions. Specific exemptions permit certain categories of records to be exempted from specific provisions of reference (a). Subsections (k)(1)-(7) of reference (a) allow exemptions for seven categories of records. To be eligible for a specific exemption, the record must meet the corresponding criteria. Note: DON PA systems of records which contain classified information automatically qualify for a (k)(1) exemption, without an established exemption rule.

(1) **(k)(1) Exemption:** Information properly classified under reference (e) and E.O. 12356, in the interest of national defense or foreign policy.

(2) **(k)(2) Exemption:** Investigatory information (other than that information within the scope of paragraph 15f(2)) compiled for law enforcement purposes. If maintaining the information causes an individual to be ineligible for or denied any right, benefit, or privilege that he or she would otherwise be eligible for or entitled to under Federal law, then he or she shall be given access to the information, except for the information that would identify a confidential source (see paragraph 15h "confidential source"). The (k)(2) exemption, when established, allows limited protection on investigative records maintained for use in personnel and administrative actions.

(3) **(k)(3) Exemption:** Records maintained in connection with providing protective services to the President of the United States and other individuals under 18 U.S.C. 3056.

(4) **(k)(4) Exemption:** Records required by Federal law to be maintained and used solely as statistical records that are not used to make any determination about an identifiable individual, except as provided by 13 U.S.C. § 8.

(5) (k)(5) **Exemption:** Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. (See paragraph 15h "confidential source"). This exemption allows protection of confidential sources in background investigations, employment inquiries, and similar inquiries used in personnel screening to determine suitability, eligibility, or qualifications.

(6) (k)(6) **Exemption:** Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service if the disclosure would compromise the objectivity or fairness of the testing or examination process.

(7) (k)(7) **Exemption:** Evaluation material used to determine potential for promotion in the military services, but only to the extent that disclosure would reveal the identity of a confidential source. (See paragraph 15h "confidential source".)

h. Confidential Source. Promises of confidentiality are to be given on a limited basis and only when essential to obtain the information sought. Establish appropriate procedures for granting confidentiality and designate those categories of individuals authorized to make such promises (see paragraph 4c for definition).

16. Enforcement Actions

a. Administrative Remedies. An individual who alleges he/she has been affected adversely by a naval activity's violation of 5 U.S.C. 552a (reference (a)) or this instruction shall be permitted to seek relief from SECNAV through proper administrative channels.

b. Civil Court Actions. After exhausting all administrative remedies, an individual may file suit in Federal court against a naval activity for any of the following acts:

(1) **Denial of an Amendment Request.** The activity head, or his/her designee wrongfully refuses the individual's request for review of the initial denial of an amendment or, after review, wrongfully refuses to amend the record;

(2) **Denial of Access.** The activity wrongfully refuses to allow the individual to review the record or wrongfully denies his/her request for a copy of the record;

(3) **Failure to Meet Recordkeeping Standards.** The activity fails to maintain an individual's record with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination about the individual's rights, benefits, or privileges and, in fact, makes an adverse determination based on the record; or

(4) **Failure to Comply with PA.** The activity fails to comply with any other provision of reference (a) or any rule or regulation promulgated under reference (a) and thereby causes the individual to be adversely affected.

c. Criminal Penalties. Subsection (i)(1) of reference (a) authorizes three criminal penalties against individuals for violations of its provisions. All three are misdemeanors punishable by fines of \$5,000.

(1) **Wrongful Disclosure.** Any member or employee of DON who, by virtue of his/her employment or position, has possession of or access to records and willfully makes a disclosure knowing that disclosure is in violation of reference (a) or this instruction.

(2) **Maintaining Unauthorized Records.** Any member or employee of DON who willfully maintains a system of records for which a notice has not been published under periodic OPNAV-NOTES 5211, subj: Current PA Issuances.

(3) **Wrongful Requesting or Obtaining Records.** Any person who knowingly and willfully requests or obtains information concerning an individual under false pretenses.

d. Litigation Status Sheet. Whenever a civil complaint citing the PA is filed against DON in Federal court or whenever criminal charges are brought against an individual in Federal court (including referral to a court-martial) for any offense listed in paragraph 16c, the responsible system manager shall promptly notify the CNO (OP-09B30) or the CMC (MI-3), as appropriate, who will then notify the Director, Defense Privacy Office, OASD(DA&M). The sample litigation status sheet contained in enclosure (14) provides a standard format for this notification. Forward a revised litigation status sheet at each stage of the litigation. When the court renders a formal disposition of the case, copies of the court's action, along with the litigation status sheet reporting the action, shall be forwarded to the CNO (OP-09B30) or the CMC (MI-3), as appropriate, who will send copies to the Defense Privacy Office.

17. Training

a. Rules of Conduct. Under subsection (e) (9) of reference (a), DON is required to establish rules of conduct for personnel dealing with PA information. In this regard, train all personnel involved in the design, development, operation, maintenance, or custody of any system of records, or in maintaining any record. Include in the training the rules of conduct and all requirements prescribed by reference (a) and this instruction, including the penalties for non-compliance. CNO (OP-09B30) and CMC (MI-3), as appropriate, shall be responsible for developing necessary training programs.

b. Types of Training. DOD has established three levels of training. This training shall be provided to persons before or shortly after assuming the duties associated with the level of involvement.

(1) **Orientation Training.** Training that provides a general understanding of this instruction to all personnel upon entering military service or civilian employment. A sample PA training package is attached at enclosure (15) for DON-wide use.

(2) **Specialized Training.** Training concerning the application of this instruction to specialized areas of job performance, i.e., personnel management, finance, medical, investigations, records management, computer systems development and operation, communications, statistical data collection and analysis, and law enforcement.

(3) **Management Training.** Training concentrated on factors affecting decisions made by managers under the PA program, such as system managers, denial authorities, PA coordinators, and managers of functions listed in paragraph 17b(2).

c. Methods of Training

(1) In developing training methods that will meet the criteria established in paragraphs 17b(2) and 17c(3), naval activities may include formal and informal (on-the-job) programs, if those personnel giving the training have, themselves, been trained.

(2) To avoid duplication and to optimize distribution and effectiveness, formal training programs shall be reviewed and coordinated with the CNO (OP-09B30) and the CMC (MI-3), as appropriate, who will coordinate these initiatives with the Defense Privacy Office.

(3) DOD, Office of Personnel Management, Association of Access Professionals (ASAP), and the Department of Agriculture Graduate School offer various kinds and levels of training. Contact CNO (OP-09B30) regarding possible course offerings.

18. PA Report

a. Report Requirements. Reference (a) requires submission of a report and assigns to the Office of Management and Budget (OMB) the responsibility for compiling the report. In addition to the report, OMB requires that agencies be prepared to report the results of the reviews specified in paragraph 7e(1)(b), upon request.

b. Responsibility

(1) CNO (OP-09B30) is responsible for preparing the consolidated DON report submission to the Defense Privacy office, who prescribes the contents and suspenses for such reports.

(2) Denial authorities at Echelon 2 commands are responsible for preparing and submitting a consolidated report for their headquarters and subordinate activities, to reach CNO (OP-09B30) by 30 March of each year. For example, the Commander in Chief, U.S. Atlantic Fleet will consolidate reports for Commander, Naval Air Force, U.S. Atlantic Fleet, Commander Patrol Wings Atlantic, etc. To accomplish that expeditiously, denial authorities at Echelon 2 commands should establish internal procedures for the rapid collection of required information.

(3) Marine Corps commanders will submit their reports to CMC (MI-3). CMC (MI-3) is responsible for submitting a consolidated report to the CNO (OP-09B30) by 30 March of each year.

(4) Denial authorities subordinate to the Echelon 2 commands will submit their consolidated reports to the Echelon 2 command by 1 March of each year. If no PA requests have been received and responded to during the reporting period, the naval activity need only advise the Echelon 2 command that they have a negative report. That can be accomplished verbally at the discretion of the Echelon 2 command.

(5) Units afloat and operational aviation squadrons who have neither received nor responded to any PA requests during the reporting period are exempt from reporting.

(6) ASN (M~~1~~RA), NJAG, and OGC are responsible for completing section B of enclosure (16), in addition to reporting any information required in section A, and submitting their report to CNO (OP-09B30) by 30 March of each year.

(7) Instructions for preparing the Annual PA Report are provided at enclosure (16). To ensure accurate reporting, naval activities should collect information on each PA request as it is worked.

c. Report Control Symbol. Unless otherwise directed, the Annual PA Report is assigned Report Control Symbol DD-DA&M(AR)1379 and is approved by DON reporting officials for three years from the date of this instruction. However, since this report is mandated by Congress, naval activities are encouraged to continue collection of statistics until notification that the report has been eliminated. The PA Report (enclosure (16)) is available from the CNO (OP-09B30), Pentagon, Washington, DC 20350-2000 or may be duplicated from the instruction. Other reporting requirements contained herein are exempt from reports control by SECNAVINST 5214.2B.

19. Staff Visits. During scheduled staff visits (i.e., command, administrative, personnel, medical, etc.), review officials shall be alert to violations of this instruction and managerial, administrative, and operational problems associated with the implementation of the PA and the DON Privacy Program.

a. Staff Visit Reporting

(1) **Initial Reports.** Enclosure (17) contains a suggested format for conducting staff visits. Document the results of findings in official reports furnished to the relevant naval officials in the chain of command. Using the sample format, indicate portions of the DON Privacy Program inspected and identify deficiencies, irregularities, and significant problems, as well as remedial actions, recommended and taken, to correct problems.

(2) **Retention of Reports.** Retain staff visit reports and follow-up reports in accordance with established records disposition standards. Make these reports available, upon request, to CNO (OP-09B30), the CMC (MI-3), or the Defense Privacy Office.

20. Computer Matching Program

a. **General.** Reference (a) and this instruction are applicable to certain types of computer matching, i.e., the computer comparison of automated systems of records. There are two specific kinds of matching programs that are fully governed by reference (a) and this instruction:

(1) Matches using records from Federal personnel or payroll systems of records as described under definitions at enclosure (18);

(2) Matches involving Federal benefit programs to accomplish one or more of the following purposes:

(a) To determine eligibility for a Federal benefit.

(b) To comply with benefit program requirements.

(c) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

The record comparison must be a computerized one. Manual comparisons are not covered, involving records from two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to reference (a)); or a DON automated systems of records and automated records maintained by a non-Federal agency (i.e., State or local government or agent thereof). A covered computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the Federal Register before the match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any. Enclosure (18) contains a detailed analysis of computer matching program procedures.

b. **Reporting.** Submit all requests for computer matching programs to CNO (OP-09B30) or the CMC (Mi-3), as appropriate, for forwarding to the Federal Register.

21. **PA Text.** A copy of The Computer Matching and Privacy Protection Act of 1988 is appended as enclosure (19).

22. Forms.

a. Privacy Act Report, OPNAV 5211/10 (Jan 92) is available from the Chief of Naval Operations (OP-09B30), Pentagon, Washington, DC 20350-2000.

b. The following forms are available in the Navy Supply System and may be requisitioned per NAVSUP P-2002D:

(1) OPNAV 5211/9 (Mar 92), Disclosure Accounting Form, S/N 0107-LF-013-8400.

(2) OPNAV 5211/12 (Mar 92), General Purpose Privacy Act Statement, S/N 0107-LF-013-8500.

DAN HOWARD
Under Secretary of the Navy

Distribution:
SNDL Parts 1 and 2
MARCORPS Codes PCN 7100000000
and 71000000100

SECNAV/OPNAV Directives Control Office
Washington Navy Yard, Building 200
Washington, DC 20374-5074 (50 copies)

Chief of Naval Operations
(Code OP-09B30)
Washington, DC 20350-2000 (300 copies)

(continues on next page)

SECNAVINST 5211.5D
17 July 1992

Chief of Naval Operations
(Code OP-09B34)
Washington, DC 20350-2000 (240 copies)

Stocked:
Navy Aviation Supply Office
Physical Distribution Division, Code 103
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (500 copies)

Table of Contents

	<u>Paragraph</u>	<u>Page</u>
Purpose	1	1
Cancellation	2	2
Applicability	3	2
Definitions	4	2
Policy	5	4
Responsibility and Authority	6	5
Chief of Naval Operations (CNO)	6a	5
Commandant of the Marine Corps (CMC)	6b	5
PA Coordinator	6c	5
Release Authority	6d	6
Denial Authority	6e	6
Review Authority	6f	6
System Manager	6g	7
DON Employees	6h	7
Systems of Records	7	7
Retrieval Practices	7a	7
Recordkeeping Standards	7b	7
Authority to Establish Systems of Records	7c	7
Exercise of First Amendment Rights	7d	8
System Manager's Evaluations and Reviews	7e	8
Discontinued Information Requirements	7f	9
Review Records Before Disclosing		
Outside the Federal Government	7g	9
Federal Government Contractors	7h	9
Applicability to Federal Government		
Contractors	7h(1)	9
Contracting procedures	7h(2)	10
Contractor compliance	7h(3)	10
Disclosing records to contractors	7h(4)	10
Safeguarding Records in Systems of Records	8	10
Minimum Standards	8a	10
Records Disposal	8b	10

Enclosure (1)

26 OCT 1992

Criteria for Creating, Altering, Amending and Deleting PA Systems of Records	9	11
Criteria for a New System of Records	9a	11
Criteria for an Alteration to a System of Records Notice	9b	11
Criteria for Amending a system of Records Notice	9c	12
Criteria for Deleting a System of Records Notice	9d	12
Collecting Information about Individuals	10	12
Collecting Directly from the Individual	10a	12
Collecting Information about Individuals from Third Persons	10b	12
Soliciting the SSN	10c	12
Contents of PAS	10d	13
Format for PAS	10e	13
Access to Records	11	14
Individual Access to Records	11a	14
Right of Access	11a(1)	14
Notification of Record's Existence	11a(2)	14
Individual Request for Access	11a(3)	14
Verifying Identity	11a(4)	14
Blanket Requests not Honored	11a(5)	14
Granting Individual Access to Records	11a(6)	15
Illegible or Incomplete Records	11a(7)	15
Access by Parents and Legal Guardians	11a(8)	15
Access to Information Compiled in Anticipation of a Civil Proceeding	11a(9)	15
Personal Notes or Records not under the Control of the DON	11a(10)	16
Relationship Between the PA and FOIA	11a(11)	16
Time Limits	11a(12)	16
Reproduction Fees	11b	16
Denying Individual Access	11c	17
Notifying the Individual	11d	17
Amendment of records	12	17
Individual Review and Amendment	12a	17
Right to Amend	12a(1)	17
In Writing	12a(2)	17
Content of Amendment Request	12a(3)	17

Enclosure (1)

26 OCT 1992

Burden of Proof	12b	18
Verifying Identity	12c	18
Limits on Amending Judicial and Quasi- Judicial Evidence and Findings	12d	18
Standards for Amendment Request Determinations	12e	18
Time Limits	12f	18
Granting an Amendment Request in Whole or in Part	12g	18
Notify the Requester	12g(1)	18
Notify Previous Recipients	12g(2)	18
Denying an Amendment Request in Whole or in Part	12h	18
Requests for Amending OPM Records	12i	18
Individual's Statement of Disagreement	12j	19
DON Statement of Reasons	12k	19
 PA Appeals	 13	 19
How to File an Appeal	13a	19
Time of Receipt	13b	19
Review Authorities	13c	19
Appeal Procedures	13d	20
Final Action, Time Limits and Documentation	13e	20
Denial of Appeal by Activity's Failure to Act	13f	20
 Disclosure of Records	 14	 20
Conditions of Disclosures	14a	20
Nonconsensual Disclosures	14b	21
Disclosures within DOD	14b(1)	21
Disclosures Required by FOIA	14b(2)	21
Disclosures for Established Routine Uses	14b(3)	23
Disclosures to the Bureau of Census	14b(4)	23
Disclosures for Statistical Research or Reporting	14b(5)	23
Disclosures to the National Archives and Records Administration	14b(6)	24
Disclosures when Requested for Law Enforcement Purposes	14b(7)	24
Disclosure to Protect the Health or Safety of an Individual	14b(8)	24
Disclosures to Congress	14b(9)	25
Disclosures to the Comptroller General for the GAO	14b(10)	25
Disclosures under Court Orders	14b(11)	25

Enclosure (1)

26 OCT 1992

Disclosures to Consumer Reporting Agencies	14b(12)	25
Disclosures to Commercial Enterprises	14c	26
Disclosure of Health Care Records to the Public	14d	26
Disclosure of Personal Information on Group/Bulk Orders	14e	26
Disclosure Accounting	14f	27
Methods of Disclosure Accounting	14g	27
Retention of Disclosure Accounting	14h	27
Exemptions	15	27
Using Exemptions	15a	27
Types of Exemptions	15b	27
General Exemptions	15b(1)	27
Specific Exemptions	15b(2)	27
Establishing Exemptions	15c	28
Exemption for Classified Material	15d	28
Exempt Records in Nonexempt Systems	15e	28
General Exemptions	15f	28
Central Intelligence Agency (CIA)	15f(1)	28
Law Enforcement	15f(2)	28
Specific Exemptions	15g	29
(k) (1)	15g(1)	29
(k) (2)	15g(2)	29
(k) (3)	15g(3)	29
(k) (4)	15g(4)	29
(k) (5)	15g(5)	30
(k) (6)	15g(6)	30
(k) (7)	15g(7)	30
Confidential Source	15h	30
Enforcement Actions	16	30
Administrative Remedies	16a	30
Civil Court Actions	16b	30
Denial of an Amendment Request	16b(1)	30
Denial of Access	16b(2)	30
Failure to Meet Recordkeeping Standards	16b(3)	30
Failure to Comply with PA	16b(4)	30
Criminal Penalties	16c	30
Wrongful Disclosure	16c(1)	30
Maintaining Unauthorized Records	16c(2)	30
Wrongful Requesting or Obtaining Records	16c(3)	30
Litigation Status Sheet	16d	31
Training	17	31
Enclosure (1)		

26 OCT 1992

Rules of Conduct	17a	31
Types of Training	17b	31
Orientation Training	17b(1)	31
Specialized Training	17b(2)	31
Management Training	17b(3)	31
Methods of Training	17c	31
PA Report	18	31
Report Requirements	18a	31
Responsibility	18b	32
Report Control Symbol	18c	32
Staff Visits	19	32
Staff Visit Reporting	19a	32
Initial Reports	19a(1)	32
Retention of Reports	19a(2)	32
Computer Matching Program	20	33
General Reporting	20a	33
	20b	33
PA Text	21	33
Forms	22	33

17 JUL 1992

**CONTENTS OF RECORD SYSTEM NOTICE AND
SAMPLE REPORT ON NEW SYSTEM OF RECORDS FORMAT**

The following contains a sample system notice. The data captions are prescribed by the Office of the Federal Register and must be included in each system notice:

a. System identification. The system identifier must appear in all system notices. It is limited to 21 positions, including DON code (i.e., NO); file number (i.e., records are categorized by a Standard Subject Identification Code (SSIC), so if you wanted to identify a military pay system of records, you would use the 7220 series); punctuation (e.g., hyphen); and sequentially numbered (e.g., NO7220-5).

b. System name

(1) The system name must indicate the general nature of the system of records and, if possible, the general category of individuals to whom it pertains.

(2) Establish acronyms parenthetically following the first use of the name (i.e., "Joint Uniform Military Pay System (JUMPS)"). Do not use acronyms unless preceded by such an explanation.

(3) The system name may not exceed 55 character positions, including punctuation and spaces.

c. System location

(1) For a system maintained in a single location, provide the exact office name, organizational identity, routing symbol, and complete mailing address.

(2) For a geographically or organizationally decentralized system, describe each level of organization or element that maintains a portion of the system of records.

(3) For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list each location.

(4) If multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are contained in an address directory published as an appendix to the DON system notices in the F.R. If the

Enclosure (2)

17 JUL 1992

addresses in the directory are incomplete, the address of each location where a portion of the record system is maintained must appear under the "system location" caption.

(5) Do not use classified addresses, but include the fact that the addresses are classified.

(6) Use the U.S. Postal Service two-letter state abbreviation and the nine-digit zip code for all domestic addresses.

d. Categories of individuals covered by the system

(1) State in clear, nontechnical terms the specific categories of individuals to whom records in the system pertain.

(2) Avoid using broad descriptions such as "all Navy personnel" or "all military personnel," unless the term actually reflects the category of individuals involved.

e. Categories of records in the system

(1) Describe in clear, nontechnical terms the types of records maintained in the system.

(2) Limit the description to documents actually retained in the system of records. Do not describe source documents that are used only to collect data and then destroyed.

(3) Remember to include each item of information that will be identified in the "Retrievability" paragraph discussed below (e.g., if you are retrieving information based on an individual's name and/or SSN, include these items in this category).

f. Authority for maintenance of the system

(1) The system of records must be authorized by a federal law or executive order of the President that permits collection of this information.

(2) When citing federal laws, include the popular names (e.g., "5 U.S.C. 552a, The Privacy Act of 1974") and for executive orders, cite the number (e.g., "Executive Order No. 9397").

(3) Cite the statute or executive order establishing the

Enclosure (2)

17 JUL 1992

naval activity. If the activity is chartered by DON Directive, cite that Directive as well as the law that authorizes the Secretary of the Navy directives.

g. Purpose(s). List the specific purpose(s) for which the system of records is maintained; i.e., the uses of the records within the activity and the rest of the DON.

h. Routine uses

(1) List all disclosures of the records outside the DOD/DON, including the recipient of the disclosed information and the uses the recipient will make of it.

(2) If possible, list the specific activity to which the record may be disclosed (e.g., "to the Veterans Administration, Office of Disability Benefits").

(3) Do not use general statements such as "to other Federal Agencies as required" or "to any other appropriate Federal Agency."

(4) Include the statement: "The 'Blanket Routine Uses' that appear at the beginning of the Department of the Navy's compilation of systems notices apply to this system," unless the individual system notice states otherwise.

i. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records

(1) Storage: State the method or methods used to store the information in the system (i.e., "maintained in computers and computer output products" or "maintained in paper files" or "maintained in paper files and in computers"). Storage does not refer to the container or facility in which the records are kept.

(2) Retrieval: Indicate how records are retrieved from the system (i.e., "by name," "by SSN," or "by name and SSN"). Ensure this same information is included under "Categories of records in the system."

(3) Safeguards: State the personnel who use the records and those responsible for protecting the records from unauthorized access. Generally identify the methods used to protect the records, such as safes, vaults, locked cabinets or rooms, guards, visitor registers, personnel screening, or computer "fail-safe" systems software. Do not describe

Enclosure (2)

17 JUL 1992

computer "fail-safe" systems software. Do not describe safeguards in such detail as to compromise system security.

(4) Retention and disposal: Indicate how long records are maintained. When appropriate, state the length of time records are maintained by the activity in an active status, when they are transferred to a Federal Records Center, how long they are kept at the Federal Records Center, and when they are transferred to the National Archives or destroyed. Ensure retention dates comply with SECNAVINST 5212.5C.

j. System manager and address

(1) List the title (not the name) and complete mailing address (including nine-digit zip code) of the official(s) responsible for managing the system of records.

(2) If the title of the specific official is unknown, such as with a local system, indicate the local commander or office head as the system manager.

k. Notification procedures

(1) Notification procedures describe how an individual can determine if a record in the system pertains to him/her.

(2) This caption shall read as follows: "Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to (Note: include complete mailing address of naval activity holding the records). The request should be signed and should include (Note: list items of retrievability, i.e., name, SSN, and address of individual concerned)."

l. Record access procedures

(1) This caption describes how an individual can review the record and obtain a copy of it.

(2) This caption shall read as follows: "Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the (Note: include complete mailing address of naval activity holding the records). The request should be signed and include full name, SSN, and address of individual concerned."

m. Contesting record procedures

Enclosure (2)

17 JUL 1992

(1) This caption describes how an individual may challenge the contents of a record that pertains to him/her.

(2) The caption shall read as follows: "The Department of the Navy rules for accessing records and contesting contents and appealing determinations by the individual concerned are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager.

n. Record source categories

(1) This caption describes who, where or what the information is usually taken from, in general terms, (i.e., specific individuals, organizations, or instructions need not be identified).

o. Exemptions claimed for the system

(1) If no exemption has been established for the system, indicate "None."

(2) If an exemption has been established, state under which provision of reference (a) it is established (i.e., "Parts of this record system may be exempt under reference (a), subsection (k)(2).").

Enclosure (2)

17 JUL 1992

-S A M P L E-

DEPARTMENT OF DEFENSE
Department of the Navy
Report on a New System Under the
Privacy Act of 1974

1. System Identification and Name: N05100-2, "Scheduled Parachute Jump Program."
2. Responsible Official: Comments on the proposed new system notice may be directed to LT John Ray, Naval Safety Center (Code 50), Naval Air Station, Norfolk, VA 23511-5796, (804) 444-6241.
3. Purpose: To track scheduled jump activity data for specific individuals or types of parachutes and correlate the information with parachute jump mishap data; analyze information to determine the relationship between various categories and combinations of jump experience and accident involvement.
To provide results of these studies to all echelons within the Navy and Marine Corps having responsibility for jump operations, parachute training, and allocation of resources to and within the parachute jump program.
To provide an annual summary of jump activity by parachute type to each reporting individual for his/her verification and personnel records. Upon request, a detailed by jump report for a specified time frame is also provided.
To provide records to the Chief of Naval Personnel for promotional screening, detailing, and compliance with minimum standards.
To provide summaries of jump activity for Marine Corps personnel to the Commandant of the Marine Corps.
To provide records of specific jump designated personnel to contractors, if required, for projects either funded by or deemed potentially valuable to the Department of the Navy.
4. Authority for Maintenance of the System: 5 U.S.C. 301, Departmental Regulations and Executive Order 9397.
5. Probable or Potential Effect(s) on Privacy of Individuals: None.
6. Relationship, if any, to other Branches of Federal Government and to State and Local Governments: None.
7. Steps Taken to Minimize the Risk of Unauthorized Access:

Enclosure (2)

17 JUL 1992

Computer area is locked after hours and access is strictly controlled. Hard drive locked to preclude unauthorized access. Only two individuals have a key to access hard drive. Building is under 24 hour watch.

8. Compatibility of each Proposed Routine Use: The "Blanket Routine Uses" set forth at the beginning of the Department of the Navy's compilation of record system notices apply to this system of records and are compatible with the purpose for which the record system was created.

9. OMB Information Collection Requirements: None have been submitted or required.

10. Supporting Documentation: There are no changes to the existing Department of the Navy procedural or exemption rules for this proposed system.

Enclosure(s)

1. Advance copy of proposed system notice for publication in the Federal Register.

Enclosure (2)

17 JUL 1992

N05100-2

System name:

Scheduled Parachute Jump Program

System location:

Naval Safety Center, Naval Air Station, Norfolk, VA 23511-5796.

Categories of individuals covered by the system:

All Navy and Marine Corps personnel and trainees who participate in the Scheduled Parachute Jump Program.

Categories of records in the system:

Unit reports of each scheduled jump, which includes name of parachutist, Social Security Number, Unit Identification Code (UIC), and model of parachute; total scheduled jump activity survey reports; and annual scheduled jump activity reports.

Authority for maintenance of the system:

5 U.S.C. § 301, Departmental Regulations and Executive Order 9397.

Purpose(s):

To track scheduled jump activity data for specific individuals or types of parachutes and correlate the information with parachute jump mishap data; analyze information to determine the relationship between various categories and combinations of jump experience and accident involvement.

To provide results of these studies to all echelons within the Navy and Marine Corps having responsibility for jump operations, parachute training, and allocation of resources to and within the parachute jump program.

To provide an annual summary of jump activity by parachute type to each reporting individual for his/her verification and personnel records. Upon request, a detailed by jump report for a specified time frame is also provided.

To provide records to the Chief of Naval Personnel for promotional screening, detailing, and compliance with minimum standards.

To provide summaries of jump activity for Marine Corps personnel to the Commandant of the Marine Corps.

To provide records of specific jump designated personnel to contractors, if required, for projects either funded by or deemed potentially valuable to the Department of the Navy.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The "Blanket Routine Uses" that appear at the beginning of the Department of the Navy's compilation of systems notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Enclosure (2)

17 JUL 1992

Magnetic tape and computer printouts.

Retrievability:

Name, Social Security Number, Unit Identification Code (UIC), and model of parachute.

Safeguards:

Computer area is locked after hours and access is strictly controlled. Hard drive locked to preclude unauthorized access. Only two individuals have a key to access hard drive. Building is under 24 hour watch.

Retention and disposal:

Permanent. Magnetic tape files contain all available records and are never purged.

System manager(s) and address:

Director of Aviation Safety Programs, Naval Safety Center, Naval Air Station, Norfolk, VA 23511-5796.

Notification procedure:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Director of Aviation Safety Programs, Naval Safety Center, Naval Air Station, Norfolk, VA 23511-5796.

The request should include full name, Social Security Number, and address of the individual concerned and should be signed.

Record access procedure:

Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Director of Aviation Safety Programs, Naval Safety Center, Naval Air Station, Norfolk, VA 23511-5796.

The request should include full name, Social Security Number, and address of the individual concerned and should be signed.

Contesting record procedure:

The Department of the Navy rules for accessing records and contesting contents and appealing determinations by the individual concerned are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager.

Record source categories:

Navy and Marine Corps jumpers.

Exemptions claimed for the system:

None.

Enclosure (2)

17 JUL 1992

**SAMPLE REPORT ON ALTERED
SYSTEM OF RECORDS NOTICE AND FORMAT**

DEPARTMENT OF DEFENSE
DEPARTMENT OF THE NAVY
REPORT ON AN ALTERED SYSTEM UNDER
THE PRIVACY ACT OF 1974

1. System Identification and Name: N05800-1, "Legal Office Litigation/Correspondence Files."
2. Responsible Official: Mr. R. Anthony McCann, Deputy Director, Litigation Office, Office of the General Counsel, Navy Department, Washington, DC 20360-5110, Telephone: (703) 602-3176.
3. Nature of Change(s) Proposed: An administrative error occurred in that the exemption rule for this system was inadvertently not codified in the CFR.
4. Authority for the Maintenance of the System: 5 U.S.C. 301, Departmental Regulations.
5. Probable or Potential Effects on the Privacy of Individuals: None.
6. Relationship of Proposal to other Branches of the Federal Government and to State and Local Government: Information in this system will be available to federal government and to state and local governments, as needed.
7. Steps Taken to Minimize Risk of Unauthorized Access:
 - a. The majority of the documents contained in this system of records consists of manual records that are maintained in file cabinets. They are kept under the control of authorized personnel during working hours. The office space in which the file cabinets are located is locked outside of official working hours.
 - b. A computerized tracking system of cases is maintained. Computer terminals are located in supervised areas. Access is controlled by password or other user code system.
 - c. A risk analysis was performed.
8. Compatibility of Proposed Routine Uses: The only routine uses for this record system are the established "blanket routine uses"

Enclosure (3)

SECNAVINST 5211.5D

17 JUL 1992

set forth at the beginning of DON record system notices. See 51 FR 18086, May 16, 1986.

9. OMB Information Collection Requirements: None have been submitted or required.

10. Supporting Documentation: Change to exemption rule is required. Copy attached.

Enclosure

1. Proposed altered record system notice for publication in the Federal Register
2. Proposed specific exemption rule for publication in the Federal Register

17 JUL 1986

N05800-1

System name: Legal Office Litigation/Correspondence Files
(51 FR 18164, May 16, 1986)

Changes:

* * * * *

Categories of individuals covered by the system: Delete entire entry and substitute with the following: "Individuals involved in litigation which requires Navy action."

Categories of records in the system: Delete the entire entry and substitute with the following: "Statements; affidavits/declarations; investigatory and administrative reports; personnel, financial, medical and business records; hotline complaints and responses thereto; discovery and discovery responses; motions; orders; rulings; letters; messages; forms; reports; surveys; audits; summons; English translations of foreign documents; photographs; legal opinions; subpoenas; pleadings; memos; related correspondence; briefs; petitions; court records involving litigation; and, related matters."

Authority for maintenance of the system: Delete the entire entry and substitute with the following: "5 U.S.C. 301, Departmental Regulations."

* * * * *

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage: At end of entry, add the following: "and computerized docket system."

Retrievability: Delete the entire entry and replace with the following: "Name of individual and the year litigation commenced."

Record source categories: Delete the entire entry and substitute with the following: "Military personnel system, medical records, investigative records, personal interviews, personal observations reported by persons witnessing or knowing of incidents."

Safeguards: Delete the entire entry and substitute with the following: "Manual records are maintained in file cabinets under the control of authorized personnel during working hours. The office space in which the file cabinets are located is locked outside of official working hours. Computer terminals are located in supervised areas. Access is controlled by password or other user code system."

Retention and disposal: Delete the entire entry and substitute with the following: "After closure, records are sent to Federal Records Center where they are retained permanently."

* * * * *

17 JUL 1992

Notification procedure: Delete the entire entry and substitute with the following: "Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the naval activity involved in the litigation or to the Associate General Counsel (Litigation), Washington, DC 20360-5110. Written requests should include name and date litigation was filed."

Record access procedures: Delete the entire entry and substitute with the following: "Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the naval activity involved in the litigation or to the Associate General Counsel (Litigation), Washington, DC 20360-5110. Written requests should include full name and year litigation commenced."

Contesting record procedures: Delete the entire entry and substitute with the following: "The Department of the Navy rules for accessing records and contesting contents and appealing initial determinations by the individual concerned are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager."

Record source categories: Delete the entire entry and substitute with the following: "Court records, records from the individual, personal interviews and statements, departmental records such as personnel files, medical records, State and Federal records, police reports and complaints, general correspondence."

Exemptions claimed for the system: Delete the entire entry and substitute with the following: "Parts of this system may be exempt under 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7) as applicable. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR Part 701, subpart G. For additional information contact the system manager."

17 JUL 1992

N05800-1

System name:

Legal Office Litigation/Correspondence Files.

System location:

Organizational elements of the Department of the Navy as indicated in the Directory of Department of the Navy Mailing Addresses.

Categories of individuals covered by the system:

Individuals involved in litigation which requires Navy action.

Categories of records in the system:

Statements; affidavits/declarations; investigatory and administrative reports; personnel, financial, medical and business records; hotline complaints and responses thereto; discovery and discovery responses; motions; orders; rulings; letters; messages; forms; reports; surveys; audits; summons; English translations of foreign documents; photographs; legal opinions; subpoenas; pleadings; memos; related correspondence; briefs; petitions; court records involving litigation; and, related matters.

Authority for maintenance of the system:

5 U.S.C. 301, Departmental Regulations.

Purpose(s):

To prepare correspondence and materials for litigation.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

The "Blanket Routine Uses" that appear at the beginning of the Department of the Navy's compilation of systems notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**Storage:**

File cabinets and computerized docket system.

Retrievability:

Name of individual and the year litigation commenced.

Safeguards:

Manual records are maintained in file cabinets under the control of authorized personnel during working hours. The office space in which the file cabinets are located is locked outside of official working hours. Computer terminals are located in supervised areas. Access is controlled by password or other user code system.

Retention and disposal:

After closure, records are sent to Federal Records Center where they are retained permanently.

17 JUL 1992

System manager(s) and address:

Associate General Counsel (Litigation), Washington, DC 20360-5110.

Notification procedure:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the naval activity involved in the litigation or to the Associate General Counsel (Litigation), Washington, DC 20360-5110. Written requests should include name and date litigation was filed.

Record access procedures:

Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the naval activity involved in the litigation or to the Associate General Counsel (Litigation), Washington, DC 20360-5110. Written requests should include full name and year litigation commenced.

Contesting record procedures:

The Department of the Navy rules for accessing records and contesting contents and appealing initial determinations by the individual concerned are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager.

Record source categories:

Court records, records from the individual, personal interviews and statements, departmental records such as personnel files, medical records, State and Federal records, police reports and complaints, general correspondence.

Exemptions claimed for the system:

Parts of this system may be exempt under 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7) as applicable. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR Part 701, subpart G. For additional information contact the system manager.

SECNAVINST 5211.5D
17 JUL 1992

CONTENTS OF AN AMENDED SYSTEMS OF RECORDS NOTICE AND FORMAT

Following is a sample of how a request to amend a systems of records should be submitted to CNO (OP-09B30) for approval and publication to the Federal Register. Consult the most current edition of OPNAVNOTE 5211 as the basis for recommended changes.

N12950-5

System name: Navy Civilian Personnel Data System (NCPDS)
(54 FR 45787, October 31, 1990)

Changes:

* * * * *

Categories of records in the system: In line 37, after the word "EPMIS" add the following, ", the Complaints Action Tracking System,".

Enclosure (4)

17 JUL 1992

N12950-5

System name:

Navy Civilian Personnel Data System (NCPDS).

System location:

Office of Civilian Personnel Management (OFFCPM) and its field offices; operating civilian personnel offices and Navy commands and management offices; and the Naval Computer and Telecommunications Station (NAVCOMTELSTA) and its designated contractors. Official mailing addresses are published as an appendix to the Department of the Navy's compilation of systems notices. Included in this notice are those records duplicated for retrievability at a site closer to where the employee works (e.g., in an administrative office or a supervisor's work area).

Categories of individuals covered by the system:

Department of the Navy civilian employees paid from appropriated and nonappropriated funds and foreign national direct and indirect hire employees.

Categories of records in the system:

The system is comprised of automated and non-automated records describing and identifying the employee (e.g., name, Social Security Number, sex, birth date, minority designator, citizenship, physical handicap code); the position occupied and the employee's qualifications; salary and salary basis or other compensation and allowances; employee's status in relation to the position occupied and the organization to which assigned; tickler dates for impending changes in status; education and training records; previous military status; functional code; previous employment record; performance appraisal and other data needed for screening and selection of an employee; referral records; professional licenses and publications; and reason for position change or other action affecting the employee and case files pertaining to EEO, MSPB, labor and employee relations, and incentive awards. The records are those found in the NCPDS subsystems: the Navy Automated Civilian Manpower Information System (NACMIS), the Training Information Management System (TIMS), the Personnel Automated Data System (PADS), the Computerized Employee Management Program Administration and Research (CEMPAR), Office of Civilian Personnel Management Customer Support Centers, the Executive Personnel Management Information System (EPMIS), the Complaints Tracking System (CATS), and the NCPDS base level and Headquarters systems.

Authority for maintenance of the system:

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 4118; E.O. 9397; 5 U.S.C. 2951; E.O. 10450; 42 U.S.C. 2000e, 5 U.S.C. 3135, 5 U.S.C. 4301, et. seq., 5 U.S.C. 4501 et. seq., 5 U.S.C. 4705 and subparts D, E, F, and G of title 5 U.S.C. and 29 CFR Part 1613 et. seq.

Purpose(s):

To manage and administer the Department's civilian personnel and civilian manpower planning programs and in the design, development, maintenance and operation of the automated system of records. Designated contractors of the Department of the Navy and Defense in the performance of their duties with respect to equipment and system design, development test, operation and maintenance.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

To the Comptroller General or any of his authorized representatives, in the course of the performance of duties of the General Accounting Office.

To the Attorney General of the United States or his authorized representatives in connection with litigation, law enforcement, or other matters under the direct jurisdiction of the Department of Justice or carried out as the legal representative of Executive Branch agencies.

To officials and employees of other departments and agencies of the Executive Branch of government upon request in the performance of their official duties related to the screening and selection of candidates for vacant positions.

To representatives of the United States Department of Labor on matters relating to the inspection, survey, audit or evaluation of the Navy's apprentice training programs or on other such matters under the jurisdiction of the Labor Department.

To representatives of the Veterans Administration on matters relating to the inspection, survey, audit or evaluation of the Navy's apprentice and on-the-job training program.

To contractors or their employees for the purpose of automated processing of data from employee personnel actions and training documents, or data collection forms and other documents.

To a duly appointed hearing examiner or arbitrator in connection with an employee's grievance.

To an appointed Administrative Judge for the purpose of conducting a hearing in connection with an employee's formal Equal Employment Opportunity (EEO) complaint.

To officials and employees of schools and other institutions engaged to provide training.

To labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

To representatives of the Federal Labor Relations Authority.

To representatives of the Merit Systems Protection Board.

The "Blanket Routine Uses" that appear at the beginning of the Department of the Navy's compilation of systems notices also apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

17 JUL 1992

Storage:

Automated records are stored on magnetic tape, disc, drum and punched cards and computer printouts. Manual records are stored in paper file folders.

Retrievability:

Information is retrieved by Social Security Number or other similar substitute if there is no Social Security Number, position number, name, or by specific employee characteristics such as date of birth, grade, occupation, employing organization, tickler dates, academic specialty level.

Safeguards:

The computer facility and terminal are accessible only to authorized persons that have been properly screened, cleared and trained. Manual and automated records and computer printouts are available only to authorized personnel having a need-to-know.

Retention and disposal:

Input documents are destroyed after data are converted to magnetic medium. Information is stored in magnetic medium within the ADP system. Information recorded via magnetic medium will be retained permanently. For TIMS and the apprentice programs the computer magnetic tapes are permanent. Manual records are maintained on a fiscal year basis and are retained for varying periods from one to five years.

System manager(s) and address:

Director, Office of Civilian Personnel Management, 800 North Quincy Street, Arlington, VA 22203-1998 and the commanding officers at the employee's activity.

Notification procedure:

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Director, Office of Civilian Personnel Management, 800 North Quincy Street, Arlington, VA 22203-1998 or to the civilian personnel officer under his/her cognizance. The request should contain the individual's full name, Social Security Number and name of employing activity. Requesters may visit the civilian personnel office at the naval activity covered by the system to obtain information. In such case, proof of identity will consist of full name, Social Security Number and a third positive identification such as a driver's license, Navy building pass or identification badge, birth certificate, Medicare card, etc. Official mailing addresses are published as an appendix to the Department of the Navy's compilation of systems of records.

Record access procedures:

Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Director, Office of Civilian Personnel Management, 800 North Quincy Street, Arlington, VA 22203-1998 or to the civilian personnel officer under his/her cognizance. The request should contain the

17 JUL 1992

individual's full name, Social Security Number and name of employing activity. Requesters may visit the civilian personnel office at the naval activity covered by the system to obtain information. In such case, proof of identity will consist of full name, Social Security Number and a third positive identification such as a driver's license, Navy building pass or identification badge, birth certificate, Medicare card, etc. Official mailing addresses are published as an appendix to the Department of the Navy's compilation of systems of records.

Contesting record procedures:

The Department of the Navy rules for accessing records and contesting contents and appealing initial determinations by the individual concerned are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager.

Record source categories:

Categories of sources of records in this system are: the civilian personnel office of the employing activity; the payroll office; OCPM headquarters; the security office of the employing activity; line managers, other designated officials and supervisors; the employee and persons named by the employee as references.

Exemptions claimed for the system:

None.

SECNAVINST 5211.5D
17 JUL 1992

CONTENTS OF A DELETED SYSTEMS OF RECORDS NOTICE AND FORMAT

Following is a sample of how a request to delete a systems of records should be submitted to CNO (OP-09B30) for approval and submission to the Federal Register. Consult the most current edition of OPNAVNOTE 5211 as the basis for recommended deletions.

N01610-5

System name: Navy Personnel Evaluation System (51 FR 18117,
May 16, 1986)

Reason: System obsolete. These kinds of records are no longer being collected and maintained. OR

System has been consolidated with NOXXXX-X (another existing system in DON inventory of systems of records).

Enclosure (5)

**SPECIAL CONSIDERATIONS FOR USING AND SAFEGUARDING
RECORDS IN COMPUTERIZED SYSTEMS OF RECORDS**

1. **PURPOSES.** This enclosure supplements from a PA standpoint, any general or overall computer security guidance issued under OPNAVINST 5239.1A. The purpose of this enclosure is to:

- a. Identify the most pressing, complex, and relevant technological advances and issues involving the PA and computer security safeguards;
- b. Illustrate several useful administrative, technical, and physical computer safeguards;
- c. Define three levels of sensitivity for records which are subject to the PA;
- d. State the responsibilities of key personnel whose duties involve automated records that are subject to the PA;
- e. List fundamental safeguards for records in computers;
- f. Specify additional safeguards for automated records that are subject to dial-up access;
- g. Provide guidance for risk analysis and management;
- h. Give guidance on the issue of personal computers and the PA;
- i. Describe the waiver system; and
- j. Indicate where additional information may be found.

2. **ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS**

a. **Statutory requirements.** Subsection (e)(10) of the PA requires the establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated hazards or threats to their security and integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

b. **Confidentiality of records.** Confidentiality of records is the status accorded records that require protection from unauthorized disclosure.

17 JUL 1992

c. Integrity of records. Integrity of records means the information in the records agrees with the source from which it is derived, and the information has not been accidentally or maliciously altered or destroyed.

d. Suggested measures. The remainder of this section lists administrative, technical, and physical measures that may be used to protect computerized records. The measures are not exhaustive, but they indicate the spectrum of available safeguards. Cost-effective choices from among the lists should be used, along with any additional measures indicated by a specific risk analysis (see paragraph 7 of this enclosure).

e. Administrative safeguards

- (1) When selecting passwords, do not use the names of relatives or friends.
- (2) Do not post passwords in work areas.
- (3) Require that passwords be changed every few months.
- (4) Quickly delete the passwords of former personnel.
- (5) Provide security awareness and training programs.
- (6) Establish contingency plans for disasters and loss of telecommunications support.
- (7) Store copies of critical records off-site.
- (8) Designate security officers for information systems.
- (9) Develop a security policy that includes criteria for determining the sensitivity of records.
- (10) Provide visible upper-management support for security.

f. Technical safeguards

- (1) Employ audit programs that log activity on computer systems.
- (2) Establish security control systems that allow different layers of access for different levels of sensitivity of records; for example, require a different password for each level of sensitivity.

(3) Label information (storage medium, screen, and printer output) to indicate PA sensitivity, such as, "PRIVACY ACT SENSITIVE," "PRIVACY ACT PROTECTED," or "PRIVACY ACT SENSITIVE - DISCLOSE ON A NEED-TO-KNOW BASIS ONLY."

(4) Encrypt records when stored or transmitted, or use an encryption code to authenticate electronic transmissions. When encryption is used, the latest federally-approved standards and procedures should be employed. Presently this means either the Data Encryption Standard (DES) or a system supplied by the National Security Agency, depending on the classification of the records and the availability of authorized secure systems. If the DES is used, FIPS-PUB-46 ("Data Encryption Standard") (NOTAL), FIPS-PUB-74 ("Guidelines for Implementing and Using the National Bureau of Standards Data Encryption Standard") (NOTAL), and FIPS-PUB-81 ("DES Modes of Operation") (NOTAL) should be followed. If a system supplied by the National Security Agency is used, the guidance from that agency should be followed.

(5) Devise techniques for user identification, ranging from simple methods such as magnetic stripe cards to more complex biometrics techniques that rely on hand or eye scanners.

(6) Employ "kernel"-based operating systems that have a central core of software that is tamperproof and controls access within the system.

(7) Use "tempest" shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment.

g. Physical safeguards

(1) Store diskettes in locked containers, or lock the room in which microcomputers are located, or do both.

(2) Install key locks for microcomputers, especially those with hard disk drives.

(3) Require special identification procedures for entry to computer rooms.

(4) Protect computer rooms from fire, water leakage, and power outages.

(5) Do not locate major computer systems near airports, loading docks, or areas prone to earthquakes or floods.

SECNAVINST 5211.5D
17 JUL 1992

3. PRIVACY ACT SECURITY LEVELS. A reasonable and productive technique for the designation of computer security levels of records that are subject to the PA is a division of three parts. When records are to be protected for the PA purposes and for other purposes, such as classified or proprietary, the highest level of protection shall be used. The three levels of sensitivity of records subject to the PA are:

a. Level 1 (low). Records required to be released under SECNAVINST 5720.42E and not used to make decisions about individuals.

b. Level 2 (medium). Ordinary personnel, medical, financial, and investigatory records and other records judged to be of comparable sensitivity.

c. Level 3 (high). Medical records, medication records, special investigatory records (identifying confidential sources, informants, undercover agents, witnesses, etc.), or other records which, if disclosed or modified improperly, could threaten an individual's life.

4. RESPONSIBILITIES OF KEY PERSONNEL. Record system managers, computer facility managers, and automated data processing (ADP) personnel (including computer security personnel) have the following responsibilities:

a. Record system manager:

(1) Certifies the sensitivity level to the computer facility manager;

(2) Checks and certifies that the reports and the DON's Federal Register notices are consistent with actual computer protection conditions; and

(3) Identifies to the computer facility manager those activities and individuals authorized to use the information, and provides prompt notification of any changes to these authorizations.

b. Computer facility manager:

(1) Informs the record system manager of the computer security options available and their costs;

(2) Considers the sensitivity of all information (all reasons for protection) when choosing overall computer security

for the facility;

(3) Maintains an inventory of all computer program applications used to process records subject to the PA and includes the identity of the systems of records involved;

(4) Verifies that requests for new programs or changes to existing programs have been published as required; and

(5) Notifies the record system manager whenever changes to computer installations or communications networks or any other changes in the ADP environment occur that require submitting an altered system report.

c. ADP personnel:

(1) Implement proper safeguards for the system;

(2) Disclose records to authorized personnel only;

(3) Adhere to the established information protection procedures and rules of conduct; and

(4) Notify the record system manager and computer facility manager whenever unauthorized personnel seek to obtain records.

5. FUNDAMENTAL SAFEGUARDS FOR RECORDS IN COMPUTERS. The following criteria apply to all three levels of sensitivity described in paragraph 3 of this enclosure.

a. Education. Education requirements include training classes, conferences, special pamphlets, computer-assisted training, films, and on-the-job training.

b. Risk analysis. Rational safeguard selection requires proper risk analysis and risk management (see paragraph 7 of this enclosure).

c. Destruction. Ensure that destroyed records cannot be reconstructed and improperly used, and that information pertaining to identifiable individuals shall not be disclosed. Records no longer required to be kept under official retention schedules should be destroyed promptly. Magnetic media may be cleared by degaussing, overwriting, or completely erasing.

d. Documentation. Notices for systems of records published in the F.R. and reports of systems forwarded to Congress and OMB

must reflect accurately the actual computer safeguards in effect.

6. SPECIAL SAFEGUARDS FOR DIAL-UP ACCESS TO PRIVACY ACT SYSTEMS

a. Protective measures. The following protective measures should be used for databanks containing PA records with sensitivity levels 2 and 3 (see paragraph 3 of this enclosure) and accessible through remote on-line terminals or personal computers:

(1) System cuts user off after three consecutive unsuccessful attempts at producing the proper password sequence;

(2) System keeps a journal (log on, accesses, etc.) and provides interactive query and report generation functions to assist in reviewing the journal;

(3) System allows access on a "need-to-know" basis with respect to databases and data elements within databases; and

(4) Information (storage medium, screen, and printer output) is labeled to indicate PA sensitivity, such as, "PRIVACY ACT SENSITIVE," "PRIVACY ACT PROTECTED," or "PRIVACY ACT SENSITIVE - DISCLOSE ON A NEED-TO-KNOW BASIS ONLY."

b. Prohibitions. The following actions should be prohibited with respect to password systems in databases containing PA records:

(1) Disclosing passwords to others;

(2) Writing or taping passwords on desks, walls, terminals, chalkboards, bulletin boards, etc. (If written down, keep password documents in sealed envelopes in locked containers.);

(3) Using the SSN as a password;

(4) Using an address, nickname, spouse's name, telephone number, birth date, or any other related information or easily-guessed numbers or letters, such as, "12345" or "abcde";

(5) Using passwords that are too short, such as, "8" or "57";

(6) Allowing a password to be seen when it is entered;

(7) Allowing a password to appear on a printout;

(8) Using a particular password for longer than 1 year (6 months for sensitive systems and less for very sensitive systems);

(9) Using a password domain of less than 10,000 possibilities (1,000,000 for sensitive systems and larger for very sensitive systems);

(10) Using the same password for access to the computer system from a terminal used to protect special databases or specific information;

(11) Using the same password for several different computer systems or databases; and

(12) Using a password after a known or suspected compromise.

7. RISK ANALYSIS AND RISK MANAGEMENT

a. OMB Requirements. OMB Circular No. A-130 (NOTAL) requires Components to perform periodic risk analyses at each installation to ensure cost-effective computer security safeguards. Note that the risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer and that management officials should use the results.

b. Measures to assist in risk analysis. The following measures should assist in risk analysis and risk management:

(1) Adopt a risk management approach in implementing security measures. Although a formal, quantitative risk analysis is required for large central computer systems and networks, this does not require formal, quantitative risk analysis procedures in all situations. For a single personal computer, a less formal, qualitative analysis might be sufficient.

(2) Consider that DON is subject to civil lawsuits for violations of the PA that cause harm to individuals.

(3) Consider the potential embarrassment to the DON for violations, the DON's responsibility to enforce the PA, and the unfairness to individuals who might suffer from violations.

(4) Include a special analysis when life-threatening situations can occur, such as when improper modifications to medical data can be fatal or when a breach of confidentiality

SECNAVINST 5211.5D
17 JUL 1992

granted to certain individuals (informants, witnesses, undercover agents, etc.) can result in serious harm or even death. This special analysis might mandate advanced technical security safeguards.

(5) Consider that computer matching programs, if not conducted properly and with stringent safeguards, can place records of millions of individuals at risk.

(6) Make a long-range plan to monitor the cost-effectiveness of the various proposed and implemented administrative, technical, and physical safeguards.

(7) Consider the reasons for protecting the integrity, confidentiality, and availability of the system, including the requirements of the PA.

(8) When necessary, seek additional assistance from the National Bureau of Standards and the National Computer Security Center.

(9) Involve management in the plan of action for protecting the system.

(10) Include the following three elements in the risk analysis:

(a) The sensitivity of information and value of assets being protected;

(b) The nature and likelihood of present and future threats, hazards, and vulnerabilities; and

(c) The cost-effectiveness of present and future safeguards.

(11) Conduct a risk analysis at least every 5 years or when there is a change to the system (hardware, software, or administrative procedures) that increases or decreases the likelihood of compromise or presents new threats to the information.

c. Protect risk analysis documents because they are potentially useful to individuals seeking unauthorized access.

d. Include a summary of the current risk analysis with any report of new or altered systems of records submitted in accordance with paragraph E.3 of chapter 7.

Enclosure (6)

e. Maintain the most recent version of the risk analysis for review by proper authorities, including the Defense Privacy Office, OMB, GAO, and congressional oversight committees.

8. THE PRIVACY ACT AND PERSONAL COMPUTERS. This section supplements, from the perspective of the PA, any general or overall guidance on personal computers issued by the DOD.

a. Personal computer (PC) security. The following items should be addressed in the policy of DON's organizations responsible for the operation of a system of records on a PC system:

(1) What actions are permissible on the PC system (what is prohibited and what records may be processed, when, and by whom);

(2) What the organization permits regarding the use of DON PCs with records off-site (use at home or while traveling on official orders);

(3) Whether personally-owned PCs may be used to do Government work;

(4) Procedures for secure maintenance of the PC;

(5) Procedures for secure operation of the PC;

(6) Procedures for the secure handling, marking, storage, and disposal of sensitive records processed by the PC;

(7) Requirement for a training program to instruct users in PC information security;

(8) Requirement that newly obtained software be tested prior to operational use to avoid software containing malicious codes that will allow unauthorized access or destroy data or programs;

(9) Feasibility of limiting the PC to a single user, which might be the most cost-effective way of securing information;

(10) Requirement that diskettes and the rooms containing PCs be locked when not in use;

(11) Possibility of using locks for PCs, especially those with hard drives;

(12) Feasibility of hardware or software packages that provide user identification, authentication, access controls, and audit trails;

(13) Consideration of computer security during procurement so that protection can be built into the PC system;

(14) Parameters of the proper risk analysis and management plan for the PCs, whether the analysis is informal-qualitative or formal-quantitative;

(15) Feasibility of requiring participation in functional end-user groups, such as medical records users, to share ideas, experience, and solutions to problems in the PA-PC security area; and

(16) If the PC is used for word processing, see enclosure (7) of this instruction.

b. Personal notes or memory joggers

(1) In some circumstances personal notes or memory joggers relating to official functions, such as a supervisor's notes, may be maintained on a PC. The conditions for maintaining them without violating the PA are: the PC must be used and completely controlled by only the author of the notes, or the PC must have security that ensures to a reasonably high degree that no one but the author has access to the notes; and the notes themselves must be used only to refresh the memory of the author.

(2) If the notes are used for official decision-making, they must be made a part of the official record within a system of records.

(3) If the notes are disclosed because other individuals have access to the PC due to inadequate security or because the author permits access to the computerized notes by others, the notes are no longer simply memory-joggers and the PA shall apply to them.

c. Prohibitions. Prior to publication in the F.R. of a notice describing the system, the report to Congress and OMB, and the elapse of the 60-day period for public comment, the following actions are prohibited:

(1) Operating a system of records on a PC;

(2) Operating a new PC-based system of records which is

17 JUL 1992

derived from combining (in whole or in part) other established systems of records;

(3) Transferring record information from a large system of records to a PC ("down-loading") to be used for new purposes; and

(4) Operating a new PC-based system of records derived from paper files from which information previously was not retrieved by personal identifiers (and thus not subject to the PA if the information will now be retrieved by personal identifiers. This situation can occur under the following circumstances:

(a) A paper-based information system contains information about individuals as well as personal identifiers but the information is not retrieved by personal identifiers and therefore is not a system of records;

(b) The system is transferred to a PC; and

(c) The PC user begins to use the individuals' identifiers to retrieve information about them, such as by using names or SSNs.

9. WAIVERS

a. Justification. The requirements of this appendix may be waived only after a showing of compelling circumstances.

b. Requesting a waiver. A request for a waiver must be submitted in writing to the Defense Privacy Office, which shall review it and make a recommendation to the Deputy Assistant Secretary of Defense (Administration), the final approval authority.

c. No waivers for the PA requirements. No waivers to any statutory requirements of the PA may be granted.

10. **ADDITIONAL INFORMATION AND RESOURCES.** Following is a list of additional sources of information and assistance not mentioned elsewhere in this instruction.

a. U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Management, Security, and Congressional Oversight, February 1986.

b. U.S. General Services Administration, Information Resources Management Service, Managing End-User Computing in the

SECNAVINST 5211.5D

17 JUL 1992

Federal Government, Number Two, September 1986.

c. U.S. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication (FIPS PUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, May 1975.

d. U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 73, Guidelines for Security of Computer Applications, June 1980

e. DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISS)," March 21, 1988

f. Title 44, United States Code, Chapter 31, "Records Management by Federal Agencies".

g. Title 44, United States Code, Chapter 33, "Disposal of Records"

h. U.S. Department of Commerce, National Bureau of Standards, Special Publication 500-137, Security for Dial-Up Lines, May 1986

i. U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 112, Password Usage, May 1985

j. National Computer Security Center, DOD Password Management Guide, April 1985

k. U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 31, Guidelines for ADP Physical Security and Risk Management, June 1974

l. U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, August 1979

m. U.S. Department of Commerce, National Bureau of Standards, Special Publication 500-120, Security of Personal Computer Systems: A Management Guide, January 1985

n. National Computer Security Center, Personal Computer Security Considerations, December 1985

o. National Computer Security Center, National Telecommunications and Information Systems Security, Advisory

Enclosure (6)

12

SECNAVINST 5211.5D
17 JUL 1992

Memorandum on Office Automation Security Guideline, NTISSAM
COMPUSEC/1-87, January 16, 1987

p. Assistant Secretary of Defense (Comptroller) Memorandum
of June 7, 1983, subject: DoD End-User Computing Policy

17 JUL 1992

**SPECIAL CONSIDERATIONS FOR SAFEGUARDING RECORDS
DURING WORD PROCESSING**

1. INTRODUCTION. Word processing support usually is provided under one of two configurations:

a. Word processing center. A word processing center, either operating independent of or within the customer's function, provides support to one or more functional areas. Typically, the customer delivers the information to be processed to the word processing center, which returns it to the customer after completion.

b. Work group. A work group consisting of word processing equipment integrated into the functional office support system. The overall word processing and functional management might be identical, and the work group will be located within or close to the functional area supported. Information flows in and out of the work group by normal office routine and the personnel are part of the office staff.

2. MINIMUM STANDARDS AND SPECIAL CONSIDERATIONS

a. Minimum standards. Regardless of the word processing configuration, afford all records subject to the PA minimum standards of protection.

b. Special Considerations. The special considerations discussed in this enclosure are intended primarily for word processing centers operating independently of the customer's function. However, managers of word processing centers and work groups operating within the customer's function should consider and adopt, when appropriate, the special considerations discussed in this enclosure (except written risk analyses in paragraph 8).

3. INFORMATION FLOW. The word processing center does not control the acquisition or ultimate use of records; therefore, only four stages of information flow will be addressed: receipt, processing, storage, and return.

4. SAFEGUARDING INFORMATION DURING RECEIPT. The word processing manager shall establish procedures that accomplish the following:

a. Customer specifies information. Require customers to indicate when information to be processed is subject to the PA. This can be done by:

- (1) Providing a check-off entry on the work request form;

Enclosure (7)

17 JUL 1992

- (2) Requiring that the work request be stamped;
- (3) Predesignating specific classes of documents, such as all personnel evaluations, all recall rosters, all personnel financial documents, etc.
- (4) Using a special cover sheet;
- (5) Requiring an audible warning on all dictation; or
- (6) Any other method which alerts the word processing personnel that the information is subject to the PA.

b. Identification by word processing personnel. Ensure that word processing personnel are capable of identifying information that is subject to the PA, in case the customer fails to do so.

5. SAFEGUARDING INFORMATION DURING PROCESSING. Word processing managers shall establish internal safeguards to protect information from compromise during the processing stage. The following measures should be considered:

a. Physical safeguards:

- (1) Controlled entry to the word processing center;
- (2) Machine configurations that eliminate the possibility of information being viewed from outside the center, such as through windows; and
- (3) Requiring that information subject to the PA be processed on designated machines.

b. Other safeguards:

- (1) Designating certain operators to process information subject to the PA;
- (2) Processing information subject to the PA only during certain times of the day;
- (3) Using only certain tapes or diskettes to process the information;
- (4) Requiring all copies of documents to be labeled indicating they contain information subject to the PA;
- (5) Returning extra copies and documents containing

Enclosure (7)

processing errors to the customer; and

(6) Disposing of waste so as to avoid compromising information.

6. SAFEGUARDING INFORMATION DURING STORAGE

a. Manager's responsibility. If information subject to the PA is to be retained at the center, ensure that it is stored properly.

b. Safeguarding measures. Consider implementing one or more of the following measures:

(1) Marking all paper copies to indicate their sensitivity;

(2) Storing media containing the information in separate areas;

(3) Marking the storage containers to indicate that their contents are sensitive;

(4) Restricting the reuse of media used to process the information or automatically erasing the media before reuse;

(5) Establishing special criteria for the retention of media used to process and store the information;

(6) Returning the media and paper copies to the customer; and

(7) If practical, discouraging long-term storage of information in any form within the center.

7. SAFEGUARDING INFORMATION DURING RETURN

a. Manager's responsibility. In conjunction with the customer, establish procedures that protect the information from the time processing is completed until the product is returned to the customer.

b. Safeguarding measures. Consider implementing one or more of the following measures:

(1) Releasing products to only designated individuals;

(2) Using sealed envelopes to transmit products to customers;

17 JUL 1992

(3) Using special cover sheets;

(4) Having word processing personnel deliver the product to the customer's location; and

(5) Using special messengers to deliver the product.

8. RISK ANALYSIS

a. **Written analysis.** Prepare a written risk analysis for each center that processes information subject to the PA.

b. **Matters to be addressed.** The analysis should address the areas discussed in paragraphs 4, 5, 6, and 7 of this enclosure, as well as any special risks that the center's location, configuration, or organization presents with respect to the compromise or alteration of information being processed or stored.

c. **Frequency of analysis.** Conduct a risk analysis at least every 5 years or whenever there is a change of equipment, configuration location, or administrative procedure that increases or decreases the likelihood of compromise or presents new threats to the information.

d. **Protecting the analysis.** Protect risk analysis documents because they are potentially useful to individuals seeking unauthorized access to the information being processed.

e. **Retaining the analysis.** Maintain the most recent version of the risk analysis for review by proper authorities.

9. SPECIAL CONSIDERATIONS IN DESIGN AND PROCUREMENT. Establish procedures to ensure that all personnel involved in the design of word processing centers and the procurement of word processing equipment are aware of the special considerations contained in this enclosure.

MICROCOMPUTER SECURITY CHECKLIST

AT THE END OF EACH DAY:

- If disks are left on desks, collect them. When staff members ask for their disks, remind them how the disks are to be stored.
- Supervise staff members who work late which is the most likely time for them to snoop in other areas.
- Supervise the cleaning staff if they work after hours in a security area.
- Ensure that all equipment not required to be left on is turned off during the night or weekend.
- Glance at all wastebaskets to ensure that reports, disks and ribbons that require special protections are not discarded improperly.
- Ensure that the data safe is closed and locked.
- Ensure that no one is hiding in bathrooms and other areas.

ONCE A MONTH:

- Remind staff to change passwords and remove old documents.
- Ensure that audit trails are being produced and reviewed.
- Ensure adequacy of backups.
- Clean drive heads, keyboards, printers and monitors to reduce maintenance.
- Ensure that programming is documented adequately.
- Ask if staff members have any questions. Untrained and confused people become frustrated and less productive, and exhibiting an interest in their work improves morale.
- Print directories to see if someone is using the equipment for unauthorized personal tasks.

17 JUL 1992

DATA STORAGE:

- Hold diskettes around the edges.
- Store them in locked containers during breaks and at night.
- Store backup diskettes in a different place.
- Do not give, sell or loan diskettes to unauthorized users.
- Create backup information regularly.
- Ensure that overhead sprinklers will not damage disks.
- Ensure that discarded reports, disks and ribbons are unreadable.

SOFTWARE SECURITY:

- Change passwords at least monthly.
- Do not tape passwords to monitors or leave them in your desk drawer.
- Do not use your name, a relative's name, your birth date, your initials, the word "password", "sex" or slang words as a password.
- Change all default passwords that come with the system or software.

GENERAL POLICIES:

- Make files with fake information for use by software consultants so that they do not use real data.
- Require that all visitors, consultants and service personnel wear badges, and escort them at all times.
- Once a year, take a complete inventory of hardware, software, manuals and chip boards.
- Assign two people to do backup to decrease the possibility of dishonesty
- Assign each disk a serial number and require staff members to sign for them.

Enclosure (7)

17 JUL 1992

- Restrict access to computer and storage areas.

COMMON SENSE PRACTICES:

- Ensure that passersby cannot view equipment. If it is placed near a window, close the curtains or blinds at the end of the day so that potential thieves are not aware of your equipment.
 - Keep cords and cables out of the way.
 - Prohibit food and drinks in the computer area.
 - Make the computer area magnet-free. There are magnets in paper clip holders, radios, telephones, dictation machines and anything with a speaker.
 - Minimize smoke and dust to the greatest extent practical.

GENERAL PURPOSE PRIVACY ACT STATEMENT

PART A - IDENTIFICATION REQUIREMENT

1. REQUIRING DOCUMENT (Describe - SECNAVINST, OPNAVNOTE, SECNAV ltr, etc.)

2. SPONSOR CODE

3. DESCRIPTIVE TITLE OF REQUIREMENT (Form title, report title, etc.)

PART B - INFORMATION TO BE FURNISHED TO INDIVIDUAL

1. AUTHORITY

2. PRINCIPLE PURPOSE(S)

3. ROUTINE USE(S)

4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION

SAMPLE

PART C - IDENTIFICATION OF FORM/REPORT/OTHER REQUIREMENT

1. FORM NO./REPORT CONTROL SYMBOL/OTHER IDENTIFICATION

PRIVACY ACT STATEMENT

17 JUL 1992

DOD BLANKET ROUTINE USES**1. ROUTINE USE - LAW ENFORCEMENT**

In the event that a system of records maintained by this Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

2. ROUTINE USE - DISCLOSURE WHEN REQUESTING INFORMATION

A record from a system of records maintained by this Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

3. ROUTINE USE - DISCLOSURE OF REQUESTED INFORMATION

A record from a system of records maintained by this Component may be disclosed to a Federal Agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. ROUTINE USE - CONGRESSIONAL INQUIRIES

Disclosure from a system of records maintained by this Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

17 JUL 1992

5. ROUTINE USE - PRIVATE RELIEF LEGISLATION

Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, may be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that circular.

6. ROUTINE USE - DISCLOSURES REQUIRED BY INTERNATIONAL AGREEMENTS

A record from a system of records maintained by this Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities in order to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of Department of Defense military and civilian personnel.

7. ROUTINE USE - DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES

Any information normally contained in IRS Form W-2 that is maintained in a record from a system of records maintained by this Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements pursuant to Title 5, U.S. Code, Sections 5516, 5517, 5520, and only to those state and local taxing authorities for which an employee or military member is or was subject to tax, regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

8. ROUTINE USE - DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT

A record from a system of records subject to the Privacy Act and maintained by this Component may be disclosed to the Office of Personnel Management concerning information on pay and leave, benefits, retirement reductions, and any other information necessary for the Office of Personnel Management to carry out its legally authorized Government-wide personnel management functions and studies.

17 JUL 1992

9. ROUTINE USE - DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION

A record from a system of records maintained by this Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

10. ROUTINE USE - DISCLOSURE TO MILITARY BANKING FACILITIES OVERSEAS

Information as to current military addresses and assignments may be provided to military banking facilities that provide banking services overseas and that are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

11. ROUTINE USE - DISCLOSURE OF INFORMATION TO THE GENERAL SERVICES ADMINISTRATION

A record from a system of records maintained by this Component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. §§ 2904 and 2906.

12. ROUTINE USE - DISCLOSURE OF INFORMATION TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

A record from a system of records maintained by this Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. §§ 2904 and 2906.

Enclosure (9)

SECNAVINST 5211.5D

17 JUL 1992

13. ROUTINE USE - DISCLOSURE TO THE MERIT SYSTEMS PROTECTION BOARD

A record from a system of records maintained by this Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel, for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation, and such other functions promulgated in 5 U.S.C. § 1205 or as may be authorized by law.

14. ROUTINE USE - COUNTERINTELLIGENCE PURPOSES

A record from a system of records maintained by this Component may be disclosed as a routine use outside the Department of Defense for the purpose of counterintelligence activities authorized by U.S. law or executive order or for the purpose of enforcing laws that protect the national security of the United States.

Enclosure (9)

17 JUL 1992

LIST OF EXEMPT SYSTEMS

1. **EXEMPTION FOR CLASSIFIED RECORDS** - All systems of records maintained by the DON shall be exempt from the requirements of the access provision of the PA (5 U.S.C. 552a(d)) under the (k)(1) exemption, to the extent that the system contains information properly classified under E.O. 12356 and that is required by that E.O. to be kept secret in the interest of national defense or foreign policy. This exemption is applicable to parts of all systems of records including those not otherwise specifically designated for exemptions herein which contain isolated items of properly classified information.

2. **EXEMPTIONS CLAIMED FOR CERTAIN NAVY PRIVACY ACT SYSTEMS OF RECORDS.**

a. **System ID and Name:** N01070-9, "White House Support Program"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4) (G) through (I), and (f).

Authority: 5 U.S.C. 552a(k) (1), (2), (3), and (5).

Reasons: Exempted portions of this system contain information which has been properly classified under E.O. 12356, and which is required to be kept secret in the interest of national defense or foreign policy. Exempted portions of this system may also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for access to classified information, and which was obtained by providing an express or implied promise to the source that his/her identity would not be revealed to the subject of the record. Exempted portions of this system may also contain information collected and maintained in connection with providing protective services to the President and other individuals protected pursuant to 18 U.S.C. 3056. Exempted portions of this system may also contain investigative records compiled for law enforcement purposes, the disclosure of which could reveal the identity of sources who provide information under an express or implied promise of confidentiality, compromise investigative techniques and procedures, jeopardize the life or physical safety of law-enforcement personnel, or otherwise interfere with enforcement proceedings or adjudications.

17 JUL 1992

b. System ID and Name: N01131-1, "Officer Selection and Appointment System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(1), (5), (6), and (7).

Reasons: Granting individuals access to portions of this system of records could result in the disclosure of classified material, or the identification of sources who provided information to the government under an express or implied promise of confidentiality. Material will be screened to permit access to unclassified material and to information that does not disclose the identity of a confidential source.

c. System ID and Name: N01133-2, "Recruiting Enlisted Selection System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(1), (5), (6), and (7).

Reasons: Granting individuals access to portions of this system of records could result in the disclosure of classified material, or the identification of sources who provided information to the government under an express or implied promise of confidentiality. Material will be screened to permit access to unclassified material and to information that does not disclose the identity of a confidential source.

d. System ID and Name: N01640-1, "Individual Correctional Records"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G) through (I), (e)(5), (e)(8), (f), and (g).

Authority: 5 U.S.C. 552a(j)(2).

Reason: Granting individuals access to portions of these records pertaining to or consisting of, but not limited to, disciplinary reports, criminal investigations, and related statements of witnesses, and such other related matter in

17 JUL 1992

conjunction with the enforcement of criminal laws, could interfere with the orderly investigations, with the orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction, or fabrication of evidence, and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by these components and could result in the invasion of the privacy of individuals only incidentally related to an investigation. The exemption of the individual's right of access to portions of these records, and the reasons therefor, necessitate the exemption of this system of records from the requirement of the other cited provisions.

e. System ID and Name: N01754-3, "Navy Child Development Services Program"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3) and (d).

Authority: 5 U.S.C. 552a(k)(2).

Reasons: Exemption is needed in order to encourage persons having knowledge of abusive or neglectful acts toward children to report such information, and to protect such sources from embarrassment or recrimination, as well as to protect their right to privacy. It is essential that the identities of all individuals who furnish information under an express promise of confidentiality be protected. Additionally, granting individuals access to information relating to criminal and civil law enforcement, as well as the release of certain disclosure accountings, could interfere with ongoing investigations and the orderly administration of justice, in that it could result in the concealment, alteration, destruction, or fabrication of information; could hamper the identification of offenders and the disposition of charges; and could jeopardize the safety and well being of parents and their children.

f. System ID and Name: N03834-1, "Special Intelligence Personnel Access File"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4) (G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(1) and (5).

17 JUL 1992

Reasons: Exempted portions of this system contain information that has been properly classified under E.O. 12356, and that is required to be kept secret in the interest of national defense or foreign policy. Exempted portions of this system also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for access to classified information and was obtained by providing an express or implied assurance to the source that his/her identity would not be revealed to the subject of the record.

g. System ID and Name: N04060-1, "Navy and Marine Corps Exchanges and Commissaries"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(4) (G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(2).

Reasons: Granting individuals access to information collected and maintained by these activities relating to the enforcement of criminal laws could interfere with orderly investigations, with orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction, or fabrication of evidence, and could also reveal and render ineffectual investigative techniques, sources, and methods used by these activities.

h. System ID and Name: N04385-1, "IG Investigatory System"

Exemption: Portions of this system or records are exempt from the following subsections of the PA: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4) (G) through (I), (e)(5), (e)(8), (f), and (g).

Authority: 5 U.S.C. 552a(j)(2)

Reasons: Granting individuals access to information collected and maintained by these activities relating to the enforcement of criminal laws could interfere with orderly investigations, the orderly administration of justice, and might enable suspects to avoid detection and apprehension. Disclosures of this information could result in the concealment, destruction, or fabrication of evidence, and possibly jeopardize the safety and well being of informants, witnesses and their families. Such disclosures could also reveal and render ineffectual

17 JUL 1992

investigatory techniques and methods and sources of information and could result in the invasion of the personal privacy of individuals only incidentally related to an investigation.

The exemption of the individual's right of access to his/her records, and the reasons therefore, necessitate the exemption of this system of records from the provisions of the other cited sections of 5 U.S.C. 552a.

i. System ID and Name: N04385-2, "Hotline Program Case File"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f).

Authority: 5 U.S.C. 552a(k) (1), (2), (5), (6) and (7).

Reasons: Exempted portions of this system consist of information compiled for the purpose of investigations, including reports of informants and investigators. Such investigations may be associated with identifiable individuals. Disclosure of files in this system would interfere with orderly investigations, and possibly result in the concealment, destruction, or fabrication of evidence, and possibly jeopardize the safety and well-being of informants, witnesses and their families. Such disclosures could also reveal and render ineffectual investigatory techniques and methods and sources of information and could further result in the invasion of the personal privacy of individuals only incidentally related to an investigation. Depending on the nature of the complaint, records may contain information that: is currently and properly classified pursuant to executive order and must be kept secret in the interest of national defense or foreign policy, is confidentially provided information located in investigatory records compiled for the purposed of enforcement of non-criminal law, relates to qualifications, eligibility, or suitability for Federal employment, is test or examination material used to determine qualifications for appointment or promotion in the Federal service, is confidentially provided information used to determine potential for promotion in the armed services.

j. System ID and Name: N05300-3, "Faculty Professional Files"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(4) (G) and (H), and (f).

17 JUL 1992

Authority: 5 U.S.C. 552a(k)(5).

Reasons: Exempted portions of this system contain information considered relevant and necessary to make a release determination as to qualifications, eligibility, or suitability for Federal employment, and was obtained by providing an express or implied promise to the source that his/her identity would not be revealed to the subject of the record.

k. System ID and Name: N05354-1, "Equal Opportunity Information Management System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(4)(G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(1) and (5).

Reasons: Granting access to information in this system of records could result in the disclosure of classified material, or reveal the identity of a source who furnished information to the Government under an express or implied promise of confidentiality. Material will be screened to permit access to unclassified material and to information that will not disclose the identity of a confidential source.

l. System ID and Name: N05520-1, "Personnel Security Eligibility Information System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(4)(G) and (I), and (f).

Authority: 5 U.S.C. 552a(k)(1), (2), (5), and (7).

Reasons: Granting individuals access to information collected and maintained in this system of records could interfere with orderly investigations; result in the disclosure of classified material; jeopardize the safety of informants, witnesses, and their families; disclose investigative techniques; and result in the invasion of privacy of individuals only incidentally related to an investigation. Material will be screened to permit access to unclassified information that will not disclose the identity of sources who provide the information to the government under an express or implied promise of confidentiality.

17 JUL 1992

m. System ID and Name: N05520-4, "NIS Investigative Files"

Exemption (1): Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G) through (I), (e)(5), (e)(8), (f), and (g).

Authority (1): 5 U.S.C. 552a(j)(2).

Reason (1): Granting individuals access to information collected and maintained by this activity relating to the enforcement of criminal laws could interfere with the orderly investigations, with the orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction, or fabrication of evidence, and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by these components and could result in the invasion of the privacy of individuals only incidentally related to an investigation. The exemption of the individual's right of access to portions of these records, and the reasons therefor, necessitate the exemption of this system of records from the requirement of the other cited provisions.

Exemption (2): Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f).

Authority (2): 5 U.S.C. 552a(k) (1), (3), (4), (5) and (6).

Reason (2): The release of disclosure accountings would permit the subject of an investigation to obtain valuable information concerning the nature of that investigation, and the information contained, or the identity of witnesses or informants, would therefor present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record. Access to the records contained in this system would inform the subject of the existence of material compiled for law enforcement purposes, the premature release of which could prevent the successful completion of investigation, and lead to the improper influencing of witnesses, the destruction of records, or the fabrication of testimony.

17 JUL 1992

Exempt portions of this system also contain information that has been properly classified under E.O. 12356, and that is required to be kept secret in the interest of national defense or foreign policy.

Exempt portions of this system also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for Federal civilian employment, military service, Federal contracts, or access to classified information, and was obtained by providing an express or implied assurance to the source that his/her identity would not be revealed to the subject of the record. The notice of this system of records published in the Federal Register sets forth the basic statutory or related authority for maintenance of the system.

The categories of sources of records in this system have been published in the Federal Register in broad generic terms. The identity of specific sources, however, must be withheld in order to protect the confidentiality of the source, of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

This system of records is exempted from procedures for notice to an individual as to the existence of records pertaining to him/her dealing with an actual or potential civil or regulatory investigation, because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation, pending or future. Mere notice of the fact of an investigation could inform the subject or others that their activities are under, or may become the subject of, an investigation. This could enable the subjects to avoid detection, to influence witnesses improperly, to destroy records, or to fabricate testimony.

Exempt portions of this system containing screening board reports. Screening board reports set forth the results of oral examination of applicants for a position as a special agent with the Naval Investigation Service Command. Disclosure of these records would reveal the areas pursued in the course of the examination and thus adversely affect the result of the selection process. Equally important, the records contain the candid views of the members composing the board. Release of the records could affect the willingness of the members to provide candid opinions and thus diminish the effectiveness of a program which is essential to maintaining the high standard of the Special Agent Corps., i.e., those records constituting examination material

26 OCT 1992

used solely to determine individual qualifications for appointment in the Federal service.

n. System ID and Name: N05520-5, "Navy Joint Adjudication (A and Clearance Systems (NJACS))"

Exemption: Portions of this system of records are exempt from the following subsections of 5 U.S.C. 552a: (d)(1-5).

Authority: 5 U.S.C. 552a(k)(1) and (k)(5).

Reasons: Granting individuals access to information collected and maintained in this system of records could result in the disclosure of classified material; and jeopardize the safety of informants, and their families. Further, the integrity of the system must be ensured so that complete and accurate records of all adjudications are maintained. Amendment could cause alteration of the record of adjudication.

o. System ID and Name: N05527-1, "Security Incident System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (c)(4), (d), (e)(2), and (3), (e)(4)(G) through (I), (e)(5), (e)(8), (f) and (g).

Authority: 5 U.S.C. 552a(j)(2).

Reasons: Granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in concealment, destruction, or fabrication of evidence, and jeopardize the safety and well being of informants, witnesses and their families, and of law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of privacy of individuals only incidentally related to an investigation.

The exemption of the individual's right of access to his/her records, and the reason therefore, necessitate the exemption of this system of records from the requirements of other cited provisions.

Enclosure (11)

26 OCT 1992

p. System ID and Name: N05527-4, "Naval Security Group Personnel Security/Access Files"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(1) through (k)(5).

Reasons: Exempt portions of this system contain information that has been properly classified under E.O. 12356, and that is required to be kept secret in the interest of national defense or foreign policy. Exempt portions of this system also contain information considered relevant and necessary to make a determination as to qualification, eligibility or suitability for access to classified special intelligence information, and that was obtained by providing an express or implied promise to the source that his/her identity would not be revealed to the subject of the record.

q. System ID and Name: N05800-1, "Legal Office Litigation/Correspondence Files"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (d), (e)(1), and (f)(2), (3), and (4).

Authority: 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7).

Reasons: Subsection (d) because granting individuals access to information relating to the preparation and conduct of litigation would impair the development and implementation of legal strategy. Accordingly, such records are exempt under the attorney-client privilege. Disclosure might also compromise on-going investigations and reveal confidential informants. Additionally, granting access to the record subject would seriously impair the Navy's ability to negotiate settlements or pursue other civil remedies. Amendment is inappropriate because the litigation files contain official records including transcripts, court orders, investigatory materials, evidentiary materials such as exhibits, decisional memorandum and other case-related papers. Administrative due process could not be achieved by the "exparte" correction of such materials.

Subsection (e)(1) because it is not possible in all instances to determine relevancy or necessity of specific information in

Enclosure (11)

the early stages of case development. What appeared relevant and necessary when collected, ultimately may be deemed unnecessary upon assessment in the context of devising legal strategy. Information collected during civil litigation investigations which is not used during subject case is often retained to provide leads in other cases or to establish patterns of activity.

Subsection (f)(2), (3), and (4) because this record system is exempt from the individual access provisions of subsection (d).

r. System ID and Name: N05819-3, "Naval Clemency and Parole Board"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(4), (d), (e)(4)(G), and (f).

Authority: 5 U.S.C. 552a(j)(2).

Reasons: Granting individuals access to records maintained by this Board could interfere with internal processes by which Board personnel are able to formulate decisions and policies with regard to clemency and parole in cases involving naval prisoners and other persons under the jurisdiction of the Board. Material will be screened to permit access to all material except such records or documents as reflect items of opinion, conclusion, or recommendation expressed by individual board members or by the board as a whole.

The exemption of the individual's right to access to portions of these records, and the reasons therefore, necessitate the partial exemption of this system of records from the requirements of the other cited provisions.

s. System ID and Name: N06320-2, "Family Advocacy Program System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3) and (d).

Authority: 5 U.S.C. 552a(k)(2) and (k)(5).

Reasons: Exemption is needed in order to encourage persons having knowledge of abusive or neglectful acts toward children to report such information, and to protect such sources from embarrassment or recriminations, as well as to protect their

Enclosure (11)

26 OCT 1992

right to privacy. It is essential that the identities of all individuals who furnish information under an express promise of confidentiality be protected. Additionally, granting individuals access to information relating to criminal and civil law enforcement, as well as the release of certain disclosure accounting, could interfere with ongoing investigations and the orderly administration of justice, in that it could result in the concealment, alteration, destruction, or fabrication of information; could hamper the identification of offenders or alleged offenders and the disposition of charges; and could jeopardize the safety and well being of parents and their children.

Exempted portions of this system also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for Federal employment and Federal contracts, and that was obtained by providing an express or implied promise to the source that his/her identity would not be revealed to the subject of the record.

t. System ID and Name: N12930-1, "Human Resources Group"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (d), (e)(4)(G) and (H), and (f).

Authority: 5 U.S.C. 552a(k)(5) and (k)(6).

Reasons: Exempted portions of this system contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for Federal employment, and was obtained by providing express or implied promise to the source that his/her identity would not be revealed to the subject of the record. Exempted portions of this system also contain test or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would comprise the objectivity or fairness of the testing or examination process.

Enclosure (11)

26 OCT 1992

3. EXEMPTIONS FOR SPECIFIC MARINE CORPS RECORD SYSTEMS.

a. System ID and Name: MMN00018, "Base Security Incident Reporting System"

Exemption: Portions of this system of records are exempt from the following subsections of the PA: (c)(3), (c)(4), (d), (e)(2) and (3), (e)(4)(G) through (I), (e)(5), (e)(8), (f), and (g).

Authority: 5 U.S.C. 552a(j)(2).

Reasons: Granting individuals access to information collected and maintained by these activities relating to the enforcement of criminal laws could interfere with orderly investigations, with the orderly administration of justice, and might enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction, or fabrication of evidence, and jeopardize the safety and well being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation.

The exemption of the individual's right of access to his/her records, and the reasons therefore, necessitate the exemption of this system of records from the requirements of other cited provisions.

b. System ID and Name: MIN00001, "Personnel and Security Eligibility and Access Information System"

Exemption: Portions of this system of records are exempt for the following subsections of the PA: (c)(3), (d), (e)(1), (e)(4)(G) through (I), and (f).

Authority: 5 U.S.C. 552a(k)(2), (k)(3), and (k)(5), as applicable.

Reasons: Exempt portions of this system contain information that has been properly classified under E.O. 12356, and that is required to be kept secret in the interest of national defense or foreign policy.

Enclosure (11)

26 OCT 1992

Exempt portions of this system also contain information considered relevant and necessary to make a determination as to qualifications, eligibility, or suitability for Federal civilian employment, military service, Federal contracts, or access to classified, compartmented, or otherwise sensitive information, and was obtained by providing an expressed or implied assurance to the source that his/her identity would not be revealed to the subject of the record.

Exempt portions of this system further contain information that identifies sources whose confidentiality must be protected to ensure that the privacy and physical safety of these witnesses and informants are protected.

17 JUL 1992

SAMPLE EXEMPTION RULE

Following is the portion of an exemption rule that must be submitted to CNO (OP-09B30) for approval and publication in the Federal Register.

ID - N05800-1

System name. Legal Office Litigation/Correspondence Files.

Exemption. Portions of this record system may be exempted from subsections of 5 U.S.C. § 552a (d), (e)(1), and (f)(2), (3) and (4).

Authority. 5 U.S.C. § 552a(k)(1), (2), (5), (6), and (7).

Reasons. Subsection (d) because granting individuals access to information relating to the preparation and conduct of litigation would impair the development and implementation of legal strategy. Accordingly, such records are exempt under the attorney-client privilege. Disclosure might also compromise on-going investigations and reveal confidential informants. Additionally, granting access to the record subject would seriously impair the Navy's ability to negotiate settlements or pursue other civil remedies. Amendment is inappropriate because the litigation files contain official records including transcripts, court orders, investigatory materials, evidentiary materials such as exhibits, decisional memorandum and other case-related papers. Administrative due process could not be achieved by the "exparte" correction of such materials.

Subsection (e)(1) because it is not possible in all instances to determine relevancy or necessity of specific information in the early stages of case development. What appeared relevant and necessary when collected, ultimately may be deemed unnecessary upon assessment in the context of devising legal strategy. Information collected during civil litigation investigations which is not used during the subject case is often retained to provide leads in other cases or to establish patterns of activity.

Subsection (f)(2), (3), and (4) because this record system is exempt from the individual access provisions of subsection (d).

Enclosure (12)

17 JUL 1992

**PROVISIONS OF THE PA FROM WHICH A
GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED**

	Subsection of the Privacy Act	Exemption	
		General	Specific
		(j) (2)	(k) (1)-(7)
(b) (1)	Disclosure within DoD -----	No	No
(b) (2)	Disclosure under FOIA -----	No	No
(b) (3)	Disclosure for a routine use ----	No	No
(b) (4)	Disclosure to Census Bureau ----	No	No
(b) (5)	Disclosure for statistics -----	No	No
(b) (6)	Disclosure to National Archives -	No	No
(b) (7)	Disclosure for law enforcement --	No	No
(b) (8)	Disclosure for health or safety -	No	No
(b) (9)	Disclosure to Congress -----	No	No
(b) (10)	Disclosure to GSA -----	No	No
(b) (11)	Disclosure pursuant to court order -----	No	No
(b) (12)	Disclosure to consumer reporting agency -----	No	No
(c) (1)	Accounting for disclosures -----	No	No
(c) (2)	Retaining disclosure accounting -	No	No
(c) (3)	Access to disclosure accounting -	Yes	Yes
(c) (4)	Informing recipients of corrections -----	Yes	No
(d) (1)	Individual access -----	Yes	Yes
(d) (2)	Amending records -----	Yes	Yes

Enclosure (13)

SECNAVINST 5211.5D
 17 JUL 1992

- | | | | |
|-------------|---|-----------|-----|
| (d) (3) | Appeal from amendment denial and
filing statement of disagreement | Yes ----- | Yes |
| (d) (4) | Disclosing statement of
disagreement ----- | Yes ----- | Yes |
| (d) (5) | Denying access to information
compiled for civil action or
proceeding ----- | Yes ----- | Yes |
| (e) (1) | Maintain only relevant and
necessary information ----- | Yes ----- | Yes |
| (e) (2) | Collect information from the
individual ----- | Yes ----- | No |
| (e) (3) | Privacy Act statement ----- | Yes ----- | No |
| (e) (4) (A) | Notice of system name and
location ----- | No ----- | No |
| (e) (4) (B) | Notice of categories of
individuals ----- | No ----- | No |
| (e) (4) (C) | Notice of categories of records | No ----- | No |
| (e) (4) (D) | Notice of routine uses ----- | No ----- | No |
| (e) (4) (E) | Notice of policies and practices | No ----- | No |
| (e) (4) (F) | Notice of system manager ----- | No ----- | No |
| (e) (4) (G) | Notice of notification
procedures ----- | Yes ----- | Yes |
| (e) (4) (H) | Notice of access procedures ---- | Yes ----- | Yes |
| (e) (4) (I) | Notice of information sources -- | Yes ----- | Yes |
| (e) (5) | Standards of accuracy ----- | Yes ----- | No |
| (e) (6) | Validating records before
disclosure ----- | No ----- | No |
| (e) (7) | No records on first
amendment activities ----- | No ----- | No |

Enclosure (13)

17 JUL 1992

(e) (8)	Notification of disclosures under legal process -----	No	-----	No
(e) (9)	Establish rules of conduct and train -----	No	-----	No
(e) (10)	Safeguarding records -----	No	-----	No
(e) (11)	Notice of new and revised routine uses -----	No	-----	No
(f) (1)	Establish rules for notification requests -----	Yes	-----	Yes
(f) (2)	Establish rules for identification -----	Yes	-----	Yes
(f) (3)	Establish rules for granting access -----	Yes	-----	Yes
(f) (4)	Establish rules for amendment requests -----	Yes	-----	Yes
(f) (5)	Establish rules for copying fees -----	Yes	-----	Yes
(g) (1)	Basis for civil lawsuits -----	Yes	-----	No
(g) (2)	Lawsuit for refusal to amend ---	Yes	-----	No
(g) (3)	Lawsuit for denial of access ---	Yes	-----	No
(g) (4)	Lawsuits for other violations --	Yes	-----	No
(g) (5)	Jurisdiction and statute of limitations -----	Yes	-----	No
(h)	Rights of parents and legal guardians -----	Yes	-----	No
(i) (1)	Criminal penalty for unauthorized disclosure -----	No	-----	No
(i) (2)	Criminal penalty for maintaining unauthorized records	No	-----	No
(i) (3)	Criminal penalty for requesting or obtaining records under false pretenses --	No	-----	No

Enclosure (13)

SECNAVINST 5211.5D
17 JUL 1992

LITIGATION STATUS REPORT

1. Case Name and Number:
2. Plaintiff(s):
3. Defendant(s):
4. Basis for Court Action:
5. Initial Litigation:
 - a. Date Complaint or Charges Filed:
 - b. Court:
 - c. Court Action:
6. Appeal (if any):
 - a. Date Appeal Filed:
 - b. Court:
 - c. Case Number:
 - d. Court Ruling:
7. Remarks:

Enclosure (14)

17 JUL 1992

SAMPLE TRAINING PACKAGE AND SLIDES

CHAPTER 1

INTRODUCTION AND DEFINITIONS

SLIDE (1) - INTRODUCTION. The Privacy Act of 1974 (Public Law 93-579) is codified as 5 U.S.C. § 552a. It should not be confused with the first subsection of the FOIA which is 5 U.S.C. § 552(a). A copy of the PA is attached at enclosure (19) of SECNAVINST 5211.5D.

SLIDE (2) - The preamble to the Act indicates the breadth of Congressional purpose of enacting that statute:

1. Individual privacy is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies.
2. The increasing use of computers and sophisticated information technology has magnified the potential for harm to privacy due to the collection, maintenance, use, and dissemination of personal information.
3. An individual's ability to obtain employment, insurance and credit, and the right to due process are endangered by misuse of information systems.
4. The right to privacy is a personal and fundamental right granted and protected by the United States Constitution.
5. To protect the privacy of individuals, it is necessary and proper for Congress to regulate the collection, maintenance, use, and dissemination of personal information by federal agencies.

SLIDE (3) - To accomplish those five purposes, the Act provides six primary features:

1. Restricts disclosure of personal information from systems of records;
2. Requires federal agencies to comply with statutory norms for collection, maintenance, use, and dissemination of personal records;
3. Provides individuals access to records about themselves;

Enclosure (15)

17 JUL 1992

4. Allows individuals to request amendments to records that are not accurate, relevant, timely, and complete;

5. Limits the use of the social security number (SSN) for identification; and

6. Provides judicial remedies, both civil and criminal, for violations of the Privacy Act.

LEGISLATIVE HISTORY. The PA resulted from two very different bills developed in the Senate and the House of Representatives.

1. The Senate bill, sponsored by Senator Sam Ervin, would have established a Federal Privacy Board with sweeping powers to oversee the collection, maintenance, use, and dissemination of personal information by federal and state agencies as well as the private sector. Most of the Senate bill's provisions did not become law; e.g., no Federal Privacy Board was created, nor were state agencies and the private sector made subject to the PA. The Senate bill defined "fair information practices", most of which were enacted and that version passed on November 21, 1974.

2. The House bill, unlike the Senate bill, had the support of the administration. The focus of the House bill was on access to and correction of records, as well as standards for data collection and maintenance. It was passed on November 21, 1974, by a 353 to 1 vote.

3. Because of the lateness of the Congressional session, both houses accepted a compromise bill negotiated by the staffs of the appropriate committees of the House and Senate. The Senate passed the compromise bill on December 17, 1974, and the House passed it the next day. It was signed by President Ford on December 31, 1974, and the PA became effective on September 27, 1975.

SLIDE (4) - FAIR INFORMATION PRACTICES. There are seven basic criteria:

1. No secret systems of records.
2. Solicit information directly from the individual.
3. Before soliciting personal information, tell the individual:
 - a. What authority permits the solicitation;

17 JUL 1992

b. Whether it is mandatory or voluntary to provide the information;

c. What the government intends to do with the information;

d. What uses will routinely be made of the information; and

e. What effects, if any, an individual's refusal to provide the requested information will have.

4. Consult the individual before providing the information to other agencies for purposes other than those for which the information was originally collected.

5. Give the individual access to information about himself or herself.

6. Allow the individual to request an amendment be made to records about him or her which are not accurate, relevant, timely, or complete.

7. Check the accuracy of information before releasing it to entities other than federal agencies.

DEFINITIONS.

1. "Agency": any executive department, military department, government-controlled corporation, independent regulatory agency, or other establishment in the executive branch, except the actual office of the President. The Act does not apply to the legislative and judicial branches of government.

2. "Individual": a citizen of the United States or an alien lawfully admitted for permanent residence.

3. "Maintain": includes maintain, collect, use, or disseminate.

4. "Record": any item, collection, or grouping of information about an individual which is maintained by an agency and which contains his or her name or other identifying particular.

5. "System of Records": a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying particular assigned

17 JUL 1992

to the individual such as a finger or voiceprint or photograph. "Under control" is intended to serve two purposes--to determine possession and to establish accountability.

6. "Statistical Record": a record in a system of records maintained solely for statistical research or reporting purposes and not used in whole or in part in making any determination about an identifiable individual except as provided by the Census Act.

7. "Routine Use": a disclosure of a record for a purpose which is compatible with the purpose for which the record was created.

8. "Matching Program": a computerized comparison of two or more automated systems of records with non-federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs.

9. "Recipient Agency": any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program.

10. "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 matching program.

11. "Source Agency": any agency which discloses records contained in a system of records to be used in a matching program, or any state or local government, or agency thereof, which discloses records to be used in a matching program.

12. "Federal Benefit Program": any 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.

13. "Federal Personnel": officers and employees of the United States government, members of the armed forces (including the reserves), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the federal government (including survivor benefits).

CHAPTER 2

CONDITIONS OF DISCLOSURE

SLIDE (5) - GENERAL RULE. The general rule is the DON shall not disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior consent of, the individual to whom the record pertains, unless one or more of the following 12 exceptions apply. They are:

1. To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties. For example, a pay clerk need not obtain your prior written consent in order to examine your pay record if such disclosure is related to the clerk's official duties, such as determining your pay entitlements. Basically, this exception was intended to authorize internal use of the record for the purpose for which the information in the record was collected, not to justify every internal agency use simply because the user works for the same department.
2. When required by the Freedom of Information Act (FOIA).
3. For a routine use. A "routine use" is defined as the use of a record for a purpose which is compatible with the purpose for which it was collected. The PA requires that each routine use be published in the Federal Register for each system of records. A disclosure under a routine use is always outside the Department of Defense activity maintaining the record.
4. To the Bureau of the Census for purposes of planning or carrying out a census or survey.
5. To a recipient who has provided the Navy with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is disclosed in a form that is not individually identifiable. This exception is limited to records which, even in combination, cannot be used to identify individuals.
6. To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States government, or for evaluation by the Archivist of the United States or his designee to determine whether the record has such value. This exception does not encompass records in a Federal Records Center

17 JUL 1992

(FRC). Navy records kept in an FRC remain under the control of this Department. The FRC acts only as an agent for the Navy.

7. To another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a criminal or civil law enforcement activity if the activity is authorized by law and if the head of the agency or instrumentality has made a written request to the agency maintaining the record specifying the particular portion desired and the law enforcement activity for which the record is sought. Blanket requests for all records of a particular type are discouraged.

8. To a person under a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.

9. To either house of Congress, or, to the extent of matters within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee. This does not authorize the disclosure of a PA record to an individual member of Congress acting in his own behalf or on the behalf of a constituent.

10. To the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office.

11. Under the order of a court of competent jurisdiction. Keep in mind, however, that a subpoena routinely issued by a court clerk is not acceptable, as it must be signed by a judge.

12. To a consumer reporting agency in accordance with section 3(d) of the Federal Claims Collection Act of 1966 [31 U.S.C. § 952(d)]. A consumer reporting agency is a person or business which assembles and evaluates information for third parties or makes/markets credit reports. A routine use must be established prior to disclosing information to a consumer reporting agency. Prior to disclosure, the agency head must determine that a valid claim exists and inform the individual: that the debt is overdue; that the agency intends to notify a consumer reporting agency; what information will be released; and that the individual may seek a full explanation of the claim, dispute the claim and appeal the initial agency decision with respect to the claim.

Only the following information may be released to the consumer reporting agency: Name, address, and SSN; amount,

SECNAVINST 5211.5D

17 JUL 1992

status, and history of the claim; and, the agency or program under which the claim arose.

17 JUL 1992

CHAPTER 3

ACCOUNTING FOR CERTAIN DISCLOSURES

SLIDE (6) - INTRODUCTION. The PA requires that we keep an accounting of disclosures made under subsection (b) so that it is simpler to trace data to be corrected, to inform individuals about disclosures made and to monitor compliance.

SLIDE (7) - CONTENT OF ACCOUNTING. The accounting must include the date, nature, and purpose of the disclosure, and the name and address of the recipient. It must be kept for 5 years after the disclosure is made or the life of the record, whichever is longer. Also, the individual must be given access to the disclosure accountings about him/her.

SLIDE (8) - EXCEPTIONS. An accounting of disclosures made between intra-agency or the FOIA need not be kept.

USES. The accounting is primarily used to: (1) allow the individual to know to whom his/her record has been disclosed; and (2) inform recipients of the corrections or amendments made under other provisions of the PA.

ACCOUNTING REQUIRED. Naval activities entitled to specific or general exemptions from the PA may exempt themselves from the requirement of access but not from the requirement of making and keeping the accounting.

17 JUL 1992

CHAPTER 4

INDIVIDUAL ACCESS TO RECORDS

A. INTRODUCTION. The DON must, upon request:

1. Inform an individual whether a system of records contains a record or records pertaining to him/her;
2. Permit an individual to review any record pertaining to him/her which is contained in a system of records;
3. Permit the individual to be accompanied by a person of his/her choosing; and
4. Permit the individual to obtain a copy of any such record in a form comprehensible to him/her at a reasonable cost.

B. DETERMINING IF A RECORD EXISTS. Upon request, we must inform an individual whether a system of records contains a record about him/her. The only exception is when the system of records has been exempted from this provision of the Act in accordance with subsections (j) and (k) which will be covered later.

C. SLIDE (9) - ACCESS BY THE INDIVIDUAL.

1. Under the PA, an individual has access to records only if those records are within a system of records; i.e., the records are retrieved by the individual's name or other identifier.

2. The individual has access to all the information in his/her record, even if it pertains to a third party.

3. The following examples illustrate some applications of the foregoing standards:

a. A record on Jane Doe filed in a system of records of all employees is retrieved and accessed by her name or SSN. Jane Doe would have the right of access to this file. This is the simplest case of a record in a system of records.

b. A reference to Jane Doe in a record about John Smith in the file of all employees is also a record within a system of records, but Jane Doe would not have the right of

17 JUL 1992

access to this file because the record is not retrieved by her name or SSN.

(1) John Smith would have access to this record, including the reference to Jane Doe, because the record is retrieved by his personal identifier.

(2) Jane Doe would have access to the information about her only if the agency has devised an indexing capability to gain access to information about her that is contained in the record of John Smith.

c. A record about Jane Doe is contained in a file about her employer, ABC Company, and the file is accessed by the name of the company rather than any individuals' names or other identifying particulars. This record is not in a system of records, and, therefore, Jane Doe would not have a right of access to it. If, in the example we just described, an indexing capability was developed and used, such a system would become a system of records to which Jane Doe would have a right of access.

4. The individual need not give a reason for wanting access, nor should the agency even ask, because the reason for the request to see the record is irrelevant.

D. ACCOMPANYING INDIVIDUALS

1. The record subject may authorize a third party to accompany him/her when viewing the record. The naval activity may require a written authorization permitting discussion of the record in the presence of the third party.

a. This provision may not be used to require individuals who request access and wish to authorize other persons to accompany them provide any reasons for the access or for the accompanying person's presence.

b. This provision is designed solely to avoid disputes over whether the individual granted permission for disclosure of information to the accompanying person.

E. PROVIDING COPIES

1. Not only does the individual have the right to review his/her record, but he/she must be provided copies in a form comprehensible to him/her.

2. We have established fees for making copies of records but not for the cost of searching for a record or reviewing it. If the only way we can allow a person to see (have access to) the record is by copying it, no fee may be charged. For instance, in order to prevent the unauthorized destruction or alteration of the record, we might choose to permit the record subject access by providing him/her with an accurate copy versus the original. Also, the original record might be on magnetic tape and the only way to provide access is to make a copy. Either way, providing access via copying is for our convenience or needs; hence, the individual must not be forced to bear the cost.

F. ACCESS TO MEDICAL DATA. Special procedures may be established for granting access to medical or psychological records pertaining to an individual. If, in our judgment, the transmission of medical information directly to a requesting individual could have an adverse effect on him/her, we should establish procedures to apprise the individual of the information without causing adverse effects. For example, the information could be transmitted to a medical doctor named by the requesting individual. Thus, while the right of individuals to have access to medical and psychological records pertaining to them is clear, the nature and circumstances of the disclosure may warrant special procedures.

G. VERIFICATION OF IDENTITY

1. We must establish requirements to verify the identity of a person requesting to see or copy his/her record, but such requirements should not be unduly burdensome. The purpose is to reasonably ensure that a person is not improperly granted access to the records of another.

2. Procedures for verifying identity, of course, will vary, depending on the nature of the records to which access is sought. For instance, no proof of identity will be required of individuals seeking access to records that are ordinarily available to any member of the public under the FOIA. On the other hand, stringent measures should be employed when the records sought are medical or other sensitive records.

3. Requests for access, when made in person, normally should require no more than such items as a building pass, identification card or driver's license. If the individual cannot provide suitable documentation, we should request a signed statement from the individual asserting his/her identity and indicating he/she understands that knowingly or willfully seeking or obtaining another person's records under false pretenses is

17 JUL 1992

punishable by a \$5,000 fine. Attorneys requesting records on behalf of a client should submit an authorization from the client.

4. If, due to the location of the records, access may be granted only by mail, verification of identity might consist of providing certain minimum identifying data, such as name or date of birth. At times, the sensitivity of the data may warrant a signed notarized statement or unsworn declaration. This is especially true where unauthorized access could cause harm or embarrassment to the individual.

H. ACKNOWLEDGING ACCESS REQUIREMENTS. The PA sets no time limits for responding to requests for access to records. However, the OMB Guidelines say that the agency "should" acknowledge the request within 10 working days and, in so doing, indicate whether access can be granted and when.

When access is to be granted, agencies normally will provide access to a record within 30 business days unless, for good cause shown, they are unable to do so, in which case the individual should be informed in writing within 30 days as to those reasons and when it is anticipated that access will be granted. A "good cause" might be that the record is inactive and stored in a record center and is not readily accessible.

I. DENYING ACCESS

1. Access may be denied only when the record is contained in a system of records which has been exempt from the access provisions of the PA under subsection (j) or (k), or when the record was compiled in reasonable anticipation of a civil action or proceeding. We'll talk about exemptions in Chapter 7.

2. While failure by the requester to identify the records or to comply with the agency's access regulations is a basis for denying access, it should not be considered a formal denial for reporting purposes. The test is whether the agency has reasonably tried to conform to the request.

J. ADMINISTRATIVE APPEALS

1. Although the PA does not provide for administrative appeals from an initial denial of access, we have established administrative appeals. One District Court has held that exhaustion of that remedy is not required before instituting a lawsuit for denial of access.

17 JUL 1992

2. The more accepted view is that, if the agency has established a procedure for administratively appealing a denial of access, the court will require the individual to exhaust that remedy before commencing a lawsuit.

K. COURT ACTIONS

1. If access is denied, both initially and after an administrative appeal, the PA provides for a civil action in federal district court.

2. The lawsuit may be filed in either of three possible jurisdictions:

- a. The district in which the complainant resides,
- b. The district in which the records are situated, or
- c. The District of Columbia.

3. The court has authority to enjoin (prohibit) the agency from withholding the documents and to order them produced.

4. The court may examine the documents before deciding whether to order them to be released to the complainant. The agency has the burden of proving its action was proper.

5. If the court finds the complainant has substantially prevailed, it may award reasonable attorney's fees and litigation costs.

L. RELATIONSHIP BETWEEN THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT

1. Who may use?

a. "FOIA": "Any person" may use the FOIA to request access to agency records. This includes U.S. citizens, permanent resident aliens, foreign nationals, corporations, unincorporated associations, universities, and state and local governments.

b. PA: Only "individuals" may use the PA. "Individual" is limited to U.S. citizens and aliens lawfully admitted for permanent residence.

17 JUL 1992

a. FOIA: The FOIA merely enables a person to obtain access to agency records.

b. PA: The PA, in addition to access, establishes a right to correct, amend, or expunge records about an individual that are not accurate, relevant, timely and complete.

3. Must the request be in writing?

a. FOIA: Yes.

b. PA: Yes.

4. What records are available?

a. FOIA: Any agency records not exempt from disclosure under one of the relatively narrow nine exemptions.

b. PA: Only records that are retrieved by the individual's personal identifier and not exempt from access under subsections (j) or (k).

5. What are the time limits?

a. FOIA: The FOIA requires that we respond to a request for access within 10 working days and to an administrative appeal within 20 working days.

b. PA: The PA does not set forth specific time limits for us to respond to a request for access, nor does it provide for an administrative appeal of a denial of access.

6. What fees may be charged?

a. FOIA: The FOIA permits an agency to charge a requester for the cost of searching for and copying the records.

b. PA: The PA permits an agency to charge only for copying, not for searching for the records.

7. Relationship of the two Acts.

a. Records that are not maintained by the requester's identifier and hence not "records" within "systems of records" are available only under the FOIA.

b. In those rare cases in which a record would be available under the PA but exempt under the FOIA, the PA applies.

17 JUL 1992

c. When a record would be available under the FOIA but exempt under the PA, the FOIA applies.

8. Under which Act should a request be processed?

a. If the request cites only the PA, and the responsive documents are contained in a system of records pertaining to the requester, the request should be processed under the PA, taking into account any exemptions available under that statute. Also, we must adhere to the fee provisions (charge only for copying), time limitations (those established by us since the statute provides none) and appeal processes (those established by the agency since the statute provides none) that are either required by the PA or by our PA regulation. Result: the requester pays less but it may take longer.

b. If the request cites only the FOIA, but the records requested are contained in a PA system of records, it should be processed under the FOIA, taking into account only those exemptions available under the PA. Also, we must adhere to the fee (charge for searching and copying), time (10 days to respond), and appeal (statutorily established) requirements of the FOIA and its own implementing regulation. Result: the requester pays more but might get faster results.

c. If the requester cites both the PA and the FOIA, we must process it under both Acts. Result: The requester gets the cheapness of the PA and the speed of the FOIA.

CHAPTER 5

AMENDMENT OF RECORDS

A. SLIDE (10) - AMENDMENT. An individual may request amendment of a record pertaining to him/her on the grounds that the record is not accurate, relevant, timely or complete. Accordingly, individuals should periodically review the personal information being maintained about them by the DON and to avail themselves of the procedures established to correct their records, as necessary.

B. REQUESTS FOR AMENDMENT. All PA systems with the exception of exempt PA systems are subject to amendment procedures. (See Chapter 7 of this training concerning exempt systems.)

1. Although the PA allows a person to request amendment, this does not mean the amendment will be automatically permitted. Further, it is incumbent upon the DON to establish procedures that individuals must follow when seeking amendment of records. Procedures, rules, and forms needed to effect amendment requests should be as simple as possible and should not be so burdensome as to discourage valid requests.

2. Requests for amendment must be in writing and the individual may be required to furnish relevant evidence to support his/her request for amendment, and such evidence naturally will depend on the record sought to be amended. For instance, the evidence needed to warrant changing a local address listing would differ from that needed to change a pay entitlement record.

3. A request for amendment should include:

- a. A description of the item or items to be amended,
- b. The specific reason for the amendment,
- c. The type of amendment action sought; e.g., expungement, correction or addition, and
- d. Copies of available documentary evidence supporting the request.

4. A request should not be denied or rejected merely because the requester failed to dot every "i" or cross every "t." On the other hand, if it is essential that certain information be

17 JUL 1992

provided or a specific format be used in order to process the request, inform the individual and allow him/her to comply without resubmitting the entire request package, if possible.

a. If the request is incomplete or unclear, allow the individual to add the needed information or to clarify the request. This might be accomplished by telephoning the requester, which certainly is not prohibited by the PA. If at all possible, the request should be reviewed in the individual's presence to determine completeness and clarity, thus perhaps saving time and some expense by both the Department of the Navy and the individual.

5. Individuals may be required to provide identification to ensure that they are indeed seeking to amend a record pertaining to themselves and not, inadvertently or intentionally, the records of others. The identification procedures shall not be used to discourage legitimate requests, to burden needlessly, nor to delay the amendment process.

6. Provisions for amending records are not intended to permit the alteration of evidence presented in the course of judicial, quasi-judicial, or quasi-legislative proceedings.

a. Any changes in such records should be made only through the established procedures consistent with the adversary process.

b. These provisions are not designed to permit collateral attack upon that which has already been the subject of a judicial or quasi-judicial action. For example, amendment provisions under the PA are not designed to permit an individual to challenge a conviction for a criminal offense received in another forum or to reopen an assessment of liability, but the individual should be able to challenge the fact that the conviction or liability has been inaccurately entered into his/her record.

7. The DoD's position and we follow it, is that the PA permits an individual to request factual amendments, but ordinarily not judgmental decisions such as efficiency/fitness reports or selection/promotion board reports.

a. Such judgmental decisions normally should be challenged before the Board for Correction of Naval Records which, by statute, is authorized to make those determinations.

17 JUL 1992

b. While factual amendments may be sought under both the PA and the procedures of the Board for Correction of Naval Records, attempts to correct other than factual matters ordinarily fall outside the provisions of the PA.

c. If a factual matter is corrected under PA procedures, any subsequent judgmental decisions affected by the factual correction, if contested, should be considered by the Board for Correction of Naval Records.

C. ACKNOWLEDGEMENT OF REQUESTS TO AMEND RECORDS

1. We have a requirement to acknowledge, in writing, the request for amendment within 10 business days. The acknowledgment should describe clearly the request and advise the individual when he or she may expect to be advised of the action taken on the request. To describe clearly the request, a copy of the request form may be appended to the acknowledgment.

2. No separate acknowledgment of receipt of the request is necessary if the request can be reviewed, processed, and the individual advised of the results of the review (whether granted or denied) within the ten-day period.

3. For requests presented in person, written acknowledgment should be provided at the time the request is presented.

D. AMENDING THE RECORD

1. The general standard for determining if a record should be amended is whether the record is accurate, relevant, timely and complete. Since we must maintain only such information about an individual that is relevant and necessary to accomplish an agency purpose, the PA contemplates "expungement and not merely redress by supplement".

2. If we agree with the individual's request to amend a record, the following steps should be taken:

a. Advise the individual;

b. Correct the record accordingly; and

c. Where an accounting of disclosures has been made, advise all previous recipients of the record that the correction was made and what the substance of the correction was. Even if there is no disclosure accounting but it is known that other DoD

17 JUL 1992

components or other federal agencies are retaining the record, notify them of the amendment.

d. If the individual requests that a specific federal agency receive notice of the amendment, comply with the request.

3. Once the amendment is accomplished, do not maintain copies of the unamended record because that would defeat the purpose of amending the record in the first place. If we agree to comply with only part of the amendment request, then the foregoing procedure should be followed with respect to the portion of the request with which there is agreement. With respect to the part of the amendment request with which we disagree, the procedure immediately following should be employed.

E. REFUSING TO AMEND THE RECORD

1. If we decide not to amend all or any part of the record as requested, the following steps should be taken:

a. Notify the individual in writing of the decision and the basis for it;

b. Inform the individual of the right to seek administrative review of the initial decision;

c. Describe the procedures for requesting an administrative review, including the name and address of the review official to whom the request must be forwarded;

d. Tell the individual where to seek assistance in filing the appeal.

2. Appeal procedures should be as simple and brief as possible and certainly not made complicated so as to discourage appeals. The agency's decision not to amend the record need not and should not be communicated to other holders of the record.

F. ADMINISTRATIVE APPEAL OF A REFUSAL TO AMEND

1. An individual who disagrees with our initial refusal to amend a record may file a request for further review of that determination.

a. The naval activity head, or someone designated in writing by the naval activity head, should undertake an independent review of the initial determination.

17 JUL 1992

b. The reviewing official should use the criteria of accuracy, relevance, timeliness and completeness discussed earlier.

c. The reviewing official may seek such additional information as is deemed necessary to make a final determination.

d. The guiding principle is to assure fairness in any determination which may be made about the individual on the basis of the record.

2. The review must be completed within 30 business days from the date on which the individual requests such review. However, for good cause shown, the head of the agency may extend the 30-day period.

G. GRANTING AN ADMINISTRATIVE APPEAL. If the reviewing official determines that the record should be amended in accordance with the individual's request, we should:

1. Advise the individual;
2. Correct the record accordingly; and
3. Inform all previous recipients of the record.

H. DENYING AN ADMINISTRATIVE APPEAL. If, after conducting a review, the official also refuses to amend the record in accordance with the individual's request, we must:

1. Advise the individual of its refusal and the reasons therefor;
2. Inform the individual of the right to file a concise statement of the his or her reasons for disagreeing with the decision of the Navy and explain the procedures for filing a statement of disagreement; and
3. Advise the individual of the right to seek judicial review of refusal to amend the record.

I. STATEMENT OF DISAGREEMENT. "Congress mandated that any individual, no matter how incredible his/her version of events, be allowed to supplement the record." If the individual elects to file a statement of disagreement, we must:

17 JUL 1992

1. Clearly annotate the portion of the record in dispute so the fact the record is disputed is apparent to anyone who subsequently might access, use or disclose it.

2. Incorporate the statement into the record.

a. For automated systems of records, the notation may consist of a special indicator on the entire record or the specific part of the record in dispute.

b. The statement of disagreement should be filed in such a manner as to permit it to be retrieved readily whenever the disputed portion of the record is to be disclosed.

c. If there is any question as to whether the dispute pertains to the information being disclosed, the statement should be included.

3. Provide copies of the statement of disagreement to all known holders of the record.

4. When the record is disclosed in the future, inform the recipient that the information is disputed and provide a copy of the individual's statement of disagreement.

J. AGENCY STATEMENT OF AGREEMENT. At its discretion, a naval activity may file a statement of its reasons for denying the request for amendment. The statement of reasons must be limited to those reasons previously furnished to the individual. Copies of the statement of reasons need not be made an integral part of the record, but must be provided to the individual upon request. The DON statement of reasons will not be subject to the amendment process unless it introduces new reasons not previously given to the individual or it is materially inaccurate.

K. JUDICIAL REVIEW. Whenever we refuse to make a requested amendment to a record and all administrative review is complete, the individual may sue in federal district court seeking to have us compelled to make the amendment. If the individual substantially prevails in court, he/she may be awarded reasonable attorney's fees and litigation costs, but no award may be made for damages.

17 JUL 1992

CHAPTER 6

AGENCY REQUIREMENTS

A. INTRODUCTION. To complement and solidify the individual interests recognized in the PA, Congress imposed explicit restrictions on the federal agencies that gather and use personal information. Together with the requirement which limits disclosure of information, the PA has a provision that governs the collection of new data and maintenance of new and existing files.

B. SLIDE (11) - MAINTAIN ONLY RELEVANT AND NECESSARY INFORMATION. Maintain only information about an individual that is relevant and necessary to accomplish a purpose of your activity and required to be accomplished by statute or E.O. of the President. We can derive authority to collect information about individuals in one of two ways: (1) By statute or E.O. of the President explicitly authorizing or directing the maintenance of a system of records; e.g., Title 13 of the United States Code with respect to the census; or (2) by statute or E.O. of the President authorizing or directing the agency to perform a function and the function in turn requires the maintenance of a system of records, e.g. 5 U.S.C. 301, Departmental Regulations. The authority to maintain a system of records does not give us the authority to maintain any information which it deems useful. The information which is maintained must be, in fact, relevant and necessary.

C. COLLECT THE INFORMATION DIRECTLY FROM THE INDIVIDUAL

1. When the information may result in adverse determinations about an individual's rights, benefits and privileges under federal programs, collect the information to the greatest extent practicable, directly from the individual. This provision requires that decisions under federal programs which effect an individual should be made on the basis of information supplied by that individual. However, the provision recognizes the practical limitations by qualifying the requirement with the words "to the greatest extent practicable". It would be "illogical" to assume that contact with third parties during an investigation is prohibited by this provision.

2. Except for certain "statistical records" which, by definition, are "not used in whole or in part in making a determination about an individual", virtually any other record

17 JUL 1992

could be used in making a determination about an individual's rights, benefits or privileges, including employment.

D. INFORMING THE INDIVIDUAL BEFORE SOLICITING INFORMATION

1. Prior to soliciting information from an individual, we must inform the individual of the following:

- a. The authority which allows the solicitation and whether providing the information is mandatory or voluntary;
- b. The principal purposes for which the information is intended;
- c. The routine use which may be made of the information;
- d. The effects, if any, of not providing the information.

This provision is intended to ensure the individual is informed of the reasons for collecting the information, how it will be used, and what the consequences are, if any, of not providing the information. This advisement is commonly referred to as the "Privacy Act Statement." We will discuss this provision more fully in Chapter 9.

E. PUBLICATION OF A NOTICE IN THE FEDERAL REGISTER

1. Upon establishing or revising a system of records, we must publish in the Federal Register a notice of the existence of the system of records. An explanation of what the notice should contain is attached at enclosure (2) of SECNAVINST 5211.5D. This public notice provision fosters Navy accountability through public scrutiny and is based on the premise that there should be no system of records whose very existence is secret.

F. RECORDS MUST BE ACCURATE, RELEVANT, TIMELY AND COMPLETE

1. Records used to make any determination about any individual must be as accurate, relevant, timely and complete as is reasonably necessary to ensure fairness to the individual. This provision was designed to minimize, if not eliminate, the risk that we will make an adverse determination about an individual on the basis of inaccurate, irrelevant, incomplete or out-of-date records that it maintains. Perfect records are not required--reasonableness is the standard.

17 JUL 1992

G. MAINTAIN NO RECORDS ON FIRST AMENDMENT ACTIVITIES.

We cannot maintain a record describing how an individual exercises First Amendment rights unless expressly authorized by statute or by the individual or unless under authorized law enforcement activity. This provision establishes a rigorous standard governing the maintenance of records regarding the exercise of First Amendment rights which include, but are not limited to, religious and political beliefs, freedom of speech and of the press, and freedom of assembly and petition.

H. NOTIFICATION FOR DISCLOSURES UNDER COMPULSORY LEGAL PROCESS

1. We must make reasonable efforts to notify an individual when his/her record is made available to any person under compulsory legal process when such process becomes a matter of public record.

2. When an order or subpoena directs that an individual's record be disclosed and the issuance of that order or subpoena is made public by the court or agency that issued it, the individual record subject must be notified. Mailing the notification to the individual's last known address is sufficient.

3. An accounting of the disclosure is also required to be made at the time the agency complies with the order or subpoena.

I. RULES OF CONDUCT FOR AGENCY PERSONNEL

1. We must establish rules and provide training for personnel engaged in using affected records.

2. All personnel who in any way have access to systems of records or who are engaged in development of procedures of systems for handling records, must be informed of the requirements of the PA and must be adequately trained in DON procedures developed to implement the Act.

J. ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS.

We must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats to their security which could result in harm, embarrassment, inconvenience or unfairness to an individual record subject. Safeguards must be tailored to the requirements of each system of records and other related requirements for security and confidentiality. A more thorough discussion of safeguards is contained in Chapter 12.

CHAPTER 7

PRIVACY ACT EXEMPTIONS

A. SLIDE (12) - INTRODUCTION. Now let's talk about the exemption provision of the PA. First, there is a special exemption from the access provisions in subsection (d)(5) that exempts information compiled in reasonable anticipation of a civil action proceeding. We'll talk about that provision later. First, let's talk about the exemptions which allow for withholding, i.e., general exemptions under subsection (j) and specific exemptions under subsection (k). What these two kinds of exemptions have in common is that they are discretionary on the part of the agency, and they are not effective until they are published in the Federal Register. A list of DON exempted systems of records is published in OPNAVNOTES 5211. The most current publication is dated _____. Also, to assist in helping you to determine what provisions of the PA can be claimed by a general or specific exemption may be claimed use the listing at enclosure (13) of SECNAVINST 5211.5D.

B. SPECIAL EXEMPTION: We are not required to grant access to any information compiled in reasonable anticipation of a civil action or proceeding. This provision has been held to be broader than the attorney work-product privilege. It covers documents prepared in anticipation of quasi-judicial administrative hearings as well as litigation.

C. GENERAL EXEMPTIONS

1. General exemptions are available for systems of records which are maintained by:

a. The Central Intelligence Agency, and

b. An agency which performs as its principal functions any activities pertaining to the enforcement of the criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon or parole authorities. Such criminal law enforcement records include criminal identification information, criminal investigation information and reports on individuals compiled at any stage from arrest or indictment through release from supervision.

c. Examples of DON activities claiming a (j) exemption are the Naval Investigative Service Command for their

17 JUL 1992

NIS Investigative Files System or any local DON activity keeping files on base security incidents.

D. SPECIFIC EXEMPTIONS. Specific exemptions focus more on the nature of the records rather than the type of agency and are available to any agency. Specific exemptions are allowed for the following types of records:

a. Records classified for national defense or foreign policy reasons.

b. Investigatory material compiled for law enforcement purposes, other than that material covered by a general exemption under subsection (j)(2). Exception: If, because of the material, any individual is denied any federal right, benefit or privilege, the material must be provided to the individual, except to the extent it would reveal the identity of a confidential source. This exemption does not include materials compiled solely for the purpose of background security investigations; or compiled for civil investigations and internal administrative investigations are, however, included in this exemption.

c. Records maintained in connection with providing protective services to the President or other specific individuals.

d. Records required to be maintained and used solely as statistical records; i.e., not used to make a determination about an identifiable individual.

e. Investigatory material compiled solely for the purpose of determining suitability, eligibility or qualification for federal civilian employment, military service, federal contracts or security clearances, but only to the extent of protecting confidential sources.

(1) We must release material in records which would not reveal the identity of a source.

(2) An individual's right to due process is not denied by withholding identities of sources even if adverse action is taken against him or her.

(3) The exemption applies equally to actions for access to records and for correction of records.

17 JUL 1992

(4) Protection of sources' identities depends upon whether the information was gathered before or after the Act became effective. After the Act went into effect, express promises of confidentiality were necessary to protect the source's identity. The identity of sources who provided information in investigations conducted before the effective date of the Act will be protected based upon an implied promise of confidentiality.

f. Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service if the disclosure would compromise the objectivity or fairness of the examination process.

g. Evaluation material used to determine potential for promotion in the armed services, but only to the extent that disclosure of the material would reveal the identity of a confidential source.

E. ESTABLISHING THE EXEMPTIONS. No system of records is automatically exempt from any provision of the PA. To obtain an exemption for a system, the head of the naval activity that maintains the system must make a determination that the system falls within one of the categories of systems which are permitted to be exempt, and submit the proposed exempted systems notice/rule to CNO (OP-09B30) for approval and subsequent publication in the Federal Register. That notice must contain the specific provisions from which the system is proposed to be exempt and why we consider the exemption necessary.

F. USING EXEMPTIONS

1. The general exemptions effectively preclude access to the records covered by them under the PA, but fairness dictates that an individual be given any access entitled by the FOIA. When dealing with exempt systems of records, the DOD supports the policy of giving the individual the maximum access, whether it be under the PA or the FOIA.

2. If a record is within an exempt system of records and the record, or a copy of it, is sent to another person or agency and that person or agency files it in a non-exempt system, a request for access through the non-exempt system will result in access being granted to the exempt record.

3. The exemption applies to the system of records for which it was established and does not travel with the record. If the status of the record changes, the exemption might be lost.

17 JUL 1992

CHAPTER 8

APPLICATION OF THE PRIVACY ACT TO CONTRACTORS

A. SLIDE (13) - INTRODUCTION. The PA provides that whenever a federal agency contracts for the operation of a system of records, the agency must cause the PA to apply to the contractor. This provision, when properly implemented, makes employees of the contractor the same as employees of the government agency in terms of liability under the PA.

B. EFFECTS OF APPLYING THE PRIVACY ACT TO CONTRACTORS.

1. The contracting agency must ensure that the relevant PA considerations are spelled out in the contract and not left to speculation.

a. "Contract" covers any contract, written or oral, but only those which provide for the operation by or for the agency of a system of records to accomplish an agency function.

b. While the contract need not have as its sole purpose the operation of a system of records, the contract normally would provide that the contractor operate such a system formally as a specific requirement of the contract.

c. There may be instances when this provision will be applicable even though the contract does not expressly provide for the operation of a system of records; e.g., when the contract can be performed only by the operation of a system of records.

2. Not only must the terms of the contract provide for the operation (as opposed to design) of a system of records, but the operation of the system must be to accomplish an agency function.

3. When a system of records is to be operated by a contractor on behalf of the Navy, the contract must specify that those records be maintained in accordance with the PA.

a. Naval activities must modify their procurement procedures and practices to ensure that all contracts are reviewed before being awarded to determine whether a system of records within the scope of the PA is being contracted for and, if so, to include appropriate language regarding the maintenance of any such systems.

17 JUL 1992

CHAPTER 9

PRIVACY ACT STATEMENTS (PASS)

A. **SLIDE (14) - INTRODUCTION.** The PA requires that, when we solicit information from an individual for a system of records, it must tell the individual five things in writing: (1) the statute or executive order of the President that authorizes the agency to solicit the information; (2) whether it is mandatory or voluntary that the individual provide the information; (3) the principal purposes for which the information is intended to be used; (4) the routine uses which may be made of the information as published in the record system notice in the Federal Register; and (5) the effects, if any, on the individual for not providing the information. This advice may be contained on the form used to solicit the information or it may be on a separate form that can be retained by the individual on request. Although not required, you may ask the individual to acknowledge in writing that they have been provided PA notice.

B. **AUTHORITY.** We should cite the specific statutory provision or E.O. of the President which authorizes the agency to collect the requested information. In some instances it might be helpful to provide a more detailed explanation of the authority. For instance, 10 U.S.C. 5031 authorizes the Secretary of the Navy to make regulations for specific DON activities and then the regulations authorize the collection of personal information for particular purposes. The PA does not require us to employ the exact language of the statute in order to give effective notice.

C. **VOLUNTARY OR MANDATORY**

1. It is mandatory for an individual to provide the information only if the statute or E.O. requires the information. Clearly if the statute or E.O. imposes a penalty for not providing the information, it is mandatory. For instance, the Internal Revenue Code requires that certain personal information be provided, and, if it is not, penalties are authorized. Unless the statute or executive order makes it mandatory, providing the information is voluntary.

2. The question of whether providing the information is mandatory or voluntary is different from the question of whether there are any effects of not providing the information. For instance, the law may not require individuals to apply for a benefit, but, for some voluntary programs, to apply without supplying certain minimal information might preclude the agency from providing the benefit.

17 JUL 1992

D. PRINCIPAL PURPOSES. The individual must be told why the information is being requested. Generally, the purposes will be related directly to the statute or E.O. previously cited as the authority for collecting the information. For instance, one of the purposes for soliciting personal information for a pay record is "to compute an individual's pay entitlements". An additional purpose might be "to withhold required and authorized deductions."

The description of the purposes must include all major purposes for which the record will be used by the naval activity or other activity outside the DON, but should not be so lengthy and detailed as to discourage the individual from reading the advisory statement. Remember, the main reason for the advice is to assist the individual in deciding whether to provide voluntary information and, when appropriate, to explain the need for mandatory information.

E. ROUTINE USES. Remember, routine use is defined as the disclosure of a record for a purpose which is compatible with the purpose for which it was collected. A routine use refers to a disclosure outside the agency that maintains the record. Also, the routine uses must be included in the public notice describing the system of records which is published in the Federal Register, and the routine uses must be established in advance by notice in the Federal Register to permit public comment.

NOTE: "Routine uses" can be distinguished from "principal purposes" in that purposes describe the objective for collecting or maintaining the information, and routine uses are the specific ways in which the information is used outside the agency that is collecting it.

a. For instance, two of the principal purposes of pay records, as mentioned earlier, could be (1) to compute the individual's pay entitlements and (2) to withhold required and authorized deductions.

b. Two of the routine uses of pay records could be (1) disclosure of pay record information to banks if the individuals have requested that their checks be sent to the banks and (2) disclosure to the Internal Revenue Service for recording withholding and Social Security information.

F. EFFECTS OF NOT PROVIDING THE INFORMATION

1. The individual must be told what, if any, effects will accrue to him/her for failure to provide the requested

17 JUL 1992

information. (The intent is to inform the individual from whom personal information is requested of the effects (both beneficial and detrimental), if any, of not providing the information.) This allows the individual to make an informed decision as to whether to provide the information on the collection form or during an interview.

2. For instance, on a form used to request annual leave, a civilian employee or service member is requested to provide personal information, and one of the effects of not providing all or part of the requested information may be that the annual leave will not be approved. NOTE: It is not mandatory that the individual provide the information in the sense that no statute or E.O. requires that the annual leave be taken nor provides a penalty for not giving the information.

3. The wording of the statement must be drafted carefully to avoid misleading or appearing to coerce the individual.

G. FORM OF THE PAS. The statement must be in writing and made available for the individual to keep if he or she so requests. When forms are used to collect personal information, the PAS may be presented in one of several methods. We have listed them in order of preference.

a. In the body of the form, preferably just below the title so that the reader will be advised before he/she begins to complete the form;

b. On the reverse side of the form with an appropriate notation under the title giving the location of the statement;

c. On a tear-off sheet attached to the form; or

d. On a separate supplement to the form.

Where similar information is collected continually, such as at check-cashing facilities, a sign containing the advice may be posted in clear view; however, if an individual requests it, a copy of the PAS must be provided to him/her. Therefore, printed copies should be available as well.

17 JUL 1992

CHAPTER 10

SOLICITATION OF SOCIAL SECURITY NUMBERS

A. SLIDE (15) - INTRODUCTION. Section 7 of the PA makes it unlawful for any federal, state or local government to deny an individual a right, benefit, or privilege provided by law because the individual refused to disclose his/her SSN.

B. EXCEPTIONS. This mandate does not apply in two types of cases: (1) when disclosure of the SSN is required by federal statute, or (2) when the system of records, whether federal, state, or local, was in existence prior to January 1, 1975, and disclosure of the SSN to verify the identity of the individual was required by a regulation or statute adopted before that date.

a. With respect to the first exception, it obviously applies to the Social Security system and federal tax system; thus an individual may be denied Social Security benefits if he/she refuses to provide his/her SSN.

b. Requiring welfare recipients to obtain and provide SSNs of children does not violate the PA because the requirement is mandated by federal statute.

C. SLIDE (16) - SOLICITING SSNs. Any federal, state, or local government agency which solicits SSNs from individuals must inform them of three things: (1) whether disclosure of the SSN is mandatory or voluntary, meaning that the statute or regulation requires disclosure of the SSN and provides penalties for failure to disclose; (2) by what statutory or other authority the SSN is solicited; (3) and what uses will be made of the SSN. (Note: President Franklin Roosevelt's Executive Order No. 9397, authorizing the widespread use of SSNs as identifiers, has been held for these purposes to be the equivalent of a federal regulation). State statutes or local ordinances may serve as the authority; however, if they were enacted after January 1, 1975, they cannot make disclosure of the SSN mandatory unless they are based on a federal statute.

D. PRACTICAL EFFECTS

1. The PA's Section 7 does not apply to demands for an individual's SSN that are mandated by statute or regulation adopted prior to January 1, 1975, for systems of records in operation prior to that date, and, of course, does not apply at all to private organizations. In short, Section 7 did no more than impose a moratorium on demands for the SSN by government

agencies under circumstances where the individual is forced to comply.

2. In the Tax Reform Act of 1976, Congress exercised its authority to authorize compulsory disclosure of the SSN for the first time since passage of the PA. That provision, designed primarily to help states locate parents who have defaulted on child support obligations and to facilitate the matching of federal and state tax returns by state authorities, opened the floodgates for mandatory disclosures of SSNs.

3. The PA's restrictions on solicitation of SSNs has had little impact on federal, state, and local government agencies.

a. Most federal agencies have been able to cite some legal authority in effect before January 1, 1975, that lets them continue to demand disclosure of the SSN.

b. Although a few state and local agencies initially abandoned the use of the SSN because they lacked such legal authority, the Tax Reform Act granted them the authority to demand the SSN for many uses.

17 JUL 1992

CHAPTER 11

SYSTEM OF RECORDS NOTICES

A. SLIDE (17) - INTRODUCTION

1. To recap, one of the key features of the PA is its prohibition against secret systems of records. Before we can begin to operate a system of records, we must publish in the Federal Register a notice of the existence of the system of records and information about that system. Not only does it serve to inform the public about each system of records, but it also serves as a guide for agency personnel who work with the systems of records. Personnel who work with a system of records should have a copy of the record system notice because it describes the key facets of the system and we are bound to operate the system within the published parameters.

B. CONTENTS OF A NOTICE FOR A SYSTEM OF RECORDS

1. SYSTEM NUMBER: This is the system identification number and it is assigned the number by CNO (OP-09B30), using the SSIC for the particular subject matter. This system number is limited to 21 characters. When you submit a systems notice to OP-09B30 for approval, this category is left blank.

2. SYSTEM NAME: This is the name assigned to the system by the submitting naval activity. The name should give some indication of the types of records in the system; e.g., "Civilian Pay Records". The system name is limited to 55 characters.

3. SYSTEM LOCATION: The address of each location where the system or a portion thereof is maintained is listed here. If the records are maintained in numerous locations, an address directory may be appended to the system notice or placed at the end of all the system notices. The DON address listing is always behind the recompilation. Always provide complete addresses with nine digit zip codes.

4. CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This lists the categories of individuals about whom records are maintained in the system; e.g., "All Navy civilian employees." By reading this heading, an individual might be able to determine if information about him/her is contained in the system.

5. CATEGORIES OF RECORDS IN THE SYSTEM: This describes the types of records maintained in the system; e.g., "individual pay records, individual leave records..." This, too, should help an

17 JUL 1992

individual determine if records about him/her are maintained in the system.

6. **AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** This identifies the federal statute or Presidential E.O. that authorizes the agency to maintain the system of records. For example, if you are collecting or retrieving by an individual's SSN, you must cite E.O. 9397, which permits this collection.

7. **PURPOSE(S):** This should explain the major purpose or purposes for maintaining the system of records, including any major uses of the records within the Department of the Navy or between components thereof. **EXAMPLE:** "To make determinations on the status of personnel regarding entitlements to pay during disability, disability benefits, severance pay, retirement pay, increases of pay for longevity, survivor's benefits, involuntary extensions of enlistments, dates of expiration of active obligated service, and accrual of annual leave."

8. **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:** This section must include all the routine uses established for the system. Remember, a routine use is a disclosure outside the agency i.e., DOD, maintaining the record for a purpose which is compatible with the purpose for which it was collected. Failure to include a particular routine use means a record cannot be used for that purpose without the individual's prior written consent. Also, certain "Blanket Routine Uses" of records have been established, and they apply to every system of records maintained within the DON.

(1) In the interest of simplicity, economy, and to avoid redundancy, these "Blanket Routine Uses" are printed at the beginning of the Navy's system notices rather than repeating them in each individual notice.

9. **POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:** Under this section the following subsections must be listed:

a. **Storage:** This describes the methods used to store the records; e.g., "...on paper in file folders, on computer tapes...".

b. **Retrievability:** This describes what personal identifiers are used to index and retrieve records in the system; e.g., "Records are retrieved by individuals' names and SSN".

17 JUL 1992

c. Safeguards: Here are listed the measures used to protect the records from unauthorized access or disclosure; e.g., "Records are stored in locked cabinets in rooms to which access is limited to those personnel who service the records."

d. Retention and disposal: This reveals the length of time the records are maintained and the means of disposal; e.g., "Records are maintained for 15 years after which they are destroyed by shredding".

10. SYSTEM MANAGER AND ADDRESS: Here is listed the title and complete mailing address of the individual responsible for implementing the policies and practices regarding the system as outlined in the notice. Please include nine-digit zip codes.

11. NOTIFICATION PROCEDURES: This describes how an individual can find out if a record pertaining to him/her is maintained in the system. This section should list the information that must be provided in order to determine whether there is a record on the individual; e.g., name, date of birth, SSN, etc. The proper verbiage for this paragraph is contained in enclosure (2) of SECNAVINST 5211.5D.

12. RECORD ACCESS PROCEDURES: This describes how individuals may obtain access to records in the system that pertains to them. This section is similar to the instructions provided in the "Notification Procedures" paragraph. Again, the proper verbiage for this paragraph is contained in enclosure (2) of SECNAVINST 5211.5D.

13. CONTESTING RECORDS PROCEDURES: This describes how individuals may challenge the contents of a record pertaining to him/her. The proper verbiage for this paragraph is contained in enclosure (2) of SECNAVINST 5211.5D.

14. RECORD SOURCE CATEGORIES: This describes who, where, or what the information is usually taken from, in general terms, (i.e., specific individuals, organizations, or instructions need not be identified), e.g., "Information is obtained from the record subjects, their previous employers,...".

15. SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT: This will list the portion of the PA that authorizes the agency to exempt the system from portions of the Act.

a. For instance, the notice for a system of criminal law enforcement records might state, "Parts of this system may be exempt under 5 U.S.C. § 552a(j)(2). For additional information,

17 JUL 1992

contact the system manager". NOTE: Listing the exemption under this section in the system notice does not establish the exemption for the system. Formal rule-making procedures under the Administrative Procedures Act must be followed.

b. If the system of records has not been exempted, this section will state, "None."

C. **RELATIONSHIP BETWEEN THE SYSTEM NOTICE AND THE PAS.** Most of the information contained in the PAS provided to individuals is contained in the record system notice. For instance, the authority, purposes and routine uses are the same for both the system notice and the PAS.

17 JUL 1992

CHAPTER 12

CONFIDENTIALITY, SECURITY, AND INTEGRITY OF RECORDS

A. SLIDE (18) - INTRODUCTION

1. The PA requires that if the DON maintains a system of records we must "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained".

2. Since systems managers are responsible for implementing the policies and practices regarding their systems of records, they are the individuals with the primary responsibility for ensuring that the established safeguards are employed. For systems of records that are dispersed geographically, the local systems managers are responsible for the part of the system that they manage, control and use.

3. The development of appropriate safeguards must be tailored to the requirements of the system as well as other factors, such as the system environment, location and accessibility. See OPNAVINST 5239.1A, "Department of the Navy Automatic Data Processing Security Program."

B. ACCESS RESTRICTIONS

1. Only those persons who have an immediate need for the records in the performance of their official duties should have unrestricted access to the record system.

2. SECNAVINST 5720.42E requires that personnel treat all unclassified records that contain personal information that normally would be withheld from the public under the privacy exemptions of the FOIA as if they were designated "For Official Use Only" and safeguard them accordingly, even if they are not actually marked "For Official Use Only."

3. At a minimum, access to records should be controlled by the following or similar practices: (a) keeping the records in areas that are not accessible to unauthorized personnel; (b) stationing personnel at key access points to control entry to the storage facility; (c) requiring identification or escorting of all visitors or wearing identification badges by authorized

17 JUL 1992

personnel; and (d) being aware when visitors are present and taking appropriate precautions.

4. The local manager or official who controls access to the records should:

a. Establish procedures for restricting access to the records so that only those personnel who have been granted formal access are allowed access without prior specific approval;

b. Provide a copy of the procedures for granting access to each person who controls access to the records; and

c. Periodically discuss the access procedures with assigned personnel to ensure complete understanding and compliance and to eliminate any weaknesses in the safeguards.

C. STORAGE REQUIREMENTS

1. Personnel responsible for records in a system of records, at a minimum, should be familiar with the storage requirements specified by the particular record system notice published in the Federal Register and should ensure those requirements are fulfilled.

2. Sensitive records, such as those relating to medical, financial, or personnel records or criminal investigations, should be kept in lockable (locked when appropriate) metal filing cabinets or in a secured room at all times when not in use during working hours and at all times during non-working hours. Each system manager should determine whether the records contained in the system of records under his/her control are sensitive to this degree.

3. Alternative storage facilities may be used, provided they furnish an equivalent or greater degree of physical security.

4. Records must not be left unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons.

D. TRANSFER OF RECORDS. Records must be transferred in a manner that prevents the accidental dissemination of information contained within them. No record from a system of records may be transmitted orally (by telephone or otherwise) to anyone until the recipient's identity and need to know are fully established.

17 JUL 1992

E. DISPOSAL OF RECORDS. Disposal and accounting of records must be in accordance with prescribed Records Retention and Disposal Schedules. Disposal of records containing personal data must be in a manner that prevents inadvertent compromise.

a. Destruction by tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding or mutilation usually are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

b. When disposing of or destroying large quantities of records containing personal information, care must be taken to ensure that the bulk of the records is maintained to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records make individually identifiable information easily available, disposal should be by one of the methods mentioned earlier such as tearing, burning, melting, pulping, etc.

F. SPECIAL CONSIDERATIONS FOR PROTECTING PERSONAL INFORMATION IN AUTOMATED SYSTEMS. The automated data processing (ADP) environment subjects personal information to special hazards with respect to unauthorized compromise, alteration, dissemination and use; hence, special considerations must be given to protecting personal information in ADP systems. At a minimum, all information subject to the PA must be processed under the procedures for information designated "For Official Use Only".

1. **SLIDE (19)** - The following factors should be considered when establishing ADP safeguards: (a) the sensitivity of the data being processed, stored and accessed; (b) the installation environment; (c) the risk of exposure; and (d) the cost of varying degrees of safeguarding.

Both intermediate and final output and storage media products containing personal information that is not classified should be labeled in such a manner as to alert those using or handling the information of the need for special protection. Either of the following labels will suffice: (a) "For Official Use Only;" or (b) "Warning: This Information Requires Protection Under the PA."

All ADP personnel involved in processing personal information must be trained in proper safeguarding procedures.

17 JUL 1992

1. Physical safeguards:

a. For all unclassified facilities, areas and devices that process information subject to the PA, establish physical safeguards that protect the information from reasonably identifiable threats that could result in unauthorized access or alteration.

b. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution, or other direct support areas that process or contain personal information subject to the PA so that access is controlled adequately.

c. Safeguard on-line devices directly coupled to ADP systems that contain or process information from systems of records to prevent unauthorized disclosure.

d. Dispose of paper records in accordance with appropriate destruction procedures.

2. Technical safeguards:

a. The use of encryption devices solely for the purpose of protecting unclassified personal information transmitted over communication circuits or during processing in computer systems normally is discouraged. However, when a comprehensive risk assessment indicates that encryption is cost-effective, it may be used.

b. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

c. Ensure that personal information is not disclosed inadvertently as residue when transferring magnetic media between activities.

d. When it is necessary to provide dial-up remote access for the processing of personal information, control access by computer-verified passwords. Change passwords periodically or whenever compromise is known or suspected.

e. Normally, passwords should give access only to those data elements (fields) required, but not to the entire data base.

f. Do not rely solely on proprietary software products to protect personal data during processing or storage.

17 JUL 1992

3. Risk Assessments: Risk assessments are required for ADP installations that process personal data. A separate risk analysis is not required for ADP installations that process classified material. A simple certification by the appropriate ADP official that the facility is cleared to process a given level of classified material and that the procedures followed in processing "For Official Use Only" material are to be followed in processing personal data subject to the PA is sufficient. For ADP installations that do not process classified material, a formal risk analysis should be prepared and the following areas should be addressed: (a) identify the specific system of records supported and determine their impact on the mission of the user, (b) identify the threats (internal, external, and natural) to the data, (c) determine the physical and operational vulnerabilities; (d) evaluate the relationship between vulnerabilities and threats, (e) assess the impact of unauthorized disclosure or modification of the personal information, (f) identify possible safeguards and their relationships to the threats to be countered. (g) analyze the economic feasibility of adopting the identified safeguards, (h) determine the safeguard to be used and develop implementation plans, (i) discuss contingency plans including operational exercise plans, (j) determine if procedures proposed are consistent with those identified in the system notices of the records concerned, and (k) include a vulnerability assessment.

The risk analysis should be reviewed by the appropriate agency officials. A risk analysis should be conducted at least every 5 years or when there is a change to the installation, its hardware, software or administrative procedures that increase or decrease the likelihood of compromise or present new threats to the information. We recommend that you protect the risk analysis document, retain a copy at the ADP installation, and make it available to appropriate inspectors and authorized personnel. A formal risk analysis should be completed at the beginning of the design phase for each new unclassified ADP installation and before beginning the processing of personal data on a regular basis in existing ADP facilities that do not process classified data.

G. SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION DURING WORD PROCESSING. Rather than going through each of the considerations at this time, I would like to refer you to enclosure (7) of SECNAVINST 5211.5D, which outlines, in detail, the standards for safeguarding word processing centers. Just keep in mind that regardless of the word processing configuration, always afford all records subject to the PA, minimum standards of protection.

17 JUL 1992

CHAPTER 13**CIVIL REMEDIES AND CRIMINAL PENALTIES****A. SLIDE (20) - INTRODUCTION - CIVIL REMEDIES**

1. The PA sets forth four agency actions for which an individual may bring a civil suit in Federal District Court:

- a. Refusal to grant access,
- b. Refusal to amend or correct a record,
- c. Failure to maintain records that are accurate, relevant, timely and complete, and
- d. Failure to comply with any other provision of the PA.

2. The lawsuits may be filed in the district where the individual resides, the district where the records are situated, or the District of Columbia.

3. All administrative remedies must be exhausted, both in access cases and in amendment cases, but not where an individual seeks damages for an agency's willful failure to maintain proper records or to comply with any other provision of the PA.

4. Only an agency may be sued in civil actions; i.e., an individual may not sue an agency official or employee personally for any of the four actions listed above.

5. The statute of limitations is 2 years; therefore, the lawsuit must be filed within 2 years from the date of the agency's refusal or failure, or within 2 years after the discovery of a willful misrepresentation by the agency that is material to its liability.

6. Reasonably incurred costs of litigation are recoverable by all PA plaintiffs who substantially prevail.

B. ACTIONS FOR REFUSAL TO GRANT ACCESS TO RECORDS

1. The District Court has authority to enjoin the agency from withholding the records and to order them produced.

2. The Court may examine the records in camera; i.e., the judge may review the records in the privacy of his or her

17 JUL 1992

chambers to determine whether the records or any portion thereof may be withheld under any of the specific exemptions under subsection (k). Remember, not only may an agency lawfully deny access or amendment to either CIA or criminal law enforcement records exempted under subsection (j), but the agency is immune from being sued in civil court because of refusal.

3. The court shall determine the matter de novo (anew).

4. The burden is on the agency to sustain its action; i.e., the agency must prove the denial of access was lawful.

5. The individual is not required to show that he/she was injured as a result of the denial of access, merely that access was wrongfully denied.

6. Damages are not recoverable.

7. If the individual prevails, the Court may

a. Order the agency to grant access to the records and

b. Order the agency to pay the individual's reasonable attorney's fees and litigation costs.

8. Attorney's fees are not recoverable for services rendered at the administrative level.

C. ACTIONS FOR REFUSAL TO AMEND OR CORRECT A RECORD

1. The Court has the power to order the amendment or correction as requested by the individual, to fashion its own amendment or correction, or to order expungement. It will determine the matter de novo.

2. The burden of proof is on the individual seeking the amendment; i.e., the individual must prove that the agency wrongfully refused to grant the request for amendment or correction.

3. If the individual prevails, the court may

a. Order that the records be amended and

b. Order the agency to pay the individual's reasonable attorney's fees and litigation costs.

17 JUL 1992

D. ACTIONS FOR FAILURE TO MAINTAIN RECORDS THAT ARE ACCURATE, RELEVANT, TIMELY AND COMPLETE

1. An individual may sue the DON for its failure to maintain records with such accuracy, relevance, timeliness and completeness as is necessary to assure fairness in any determination about the individual that may be made on the basis of such record IF, in fact, an adverse determination IS made.

a. Unlike the actions for refusal to grant access or amendment, these actions require that the individual show that he/she was adversely affected by the agency's failure to maintain proper records.

b. The individual must prove that the adverse effect was directly caused by the improper record. An adverse effect would be a loss or denial of a right, benefit or privilege to which the individual would otherwise be entitled.

c. Perfect records are not required. Reasonableness is the standard. An agency will not be strictly liable for inaccuracies.

2. Additionally, to obtain damages, the individual must show that the DON's action was intentional and willful.

3. If the individual successfully proves his/her case, he/she is entitled to

a. Actual damages sustained as a result of the agency's action, but in no case less than \$1,000, and

b. Reasonable attorney's fees and litigation costs.

E. ACTIONS FOR VIOLATIONS OF ANY OTHER PROVISIONS OF THE PA

1. An individual may sue the DON if it fails to comply with any other provision of the PA in such a way as to have an adverse effect on the individual.

a. As was discussed in paragraph D above, the individual must prove

(1) That he/she was adversely affected and

(2) That the adverse effect was directly caused by the DON's violation of the PA.

17 JUL 1992

b. Here, too, the individual must show that the our action was intentional and willful.

2. If the individual wins, he/she is entitled to

a. Actual damages sustained as a result of the DON's violation, but in no case less than \$1,000, and

b. Reasonable attorney's fees and litigation costs.

F. CRIMINAL PENALTIES

1. Any agency official or employee who willfully does either of the following is punishable for a misdemeanor and may be fined up to \$5,000:

a. Makes a disclosure of a record knowing it to be in violation of the PA, or

b. Maintains a system of records without having published a system notice in the Federal Register.

2. Any person who knowingly and willfully requests or obtains a record of another individual from the DON under false pretenses is punishable for a misdemeanor and may be fined up to \$5,000.

SLIDE 1



DEPARTMENT OF THE NAVY
TRAINING ON THE
PRIVACY ACT OF 1974

WHY WAS ACT PASSED?

- **INDIVIDUAL PRIVACY AFFECTED**
- **INCREASING USE OF COMPUTERS**
- **MISUSE OF INFORMATION SYSTEMS**
- **RIGHT OF PRIVACY IS RIGHT PROTECTED BY CONSTITUTION**
- **CONGRESS NEEDED TO REGULATE COLLECTION, MAINTENANCE, USE AND DISSEMINATION OF PERSONAL INFORMATION**

SLIDE 3

FEATURES OF THE ACT

- **RESTRICTS DISCLOSURE**
- **REQUIRES FEDERAL AGENCIES TO COMPLY**
- **ALLOWS INDIVIDUALS ACCESS TO RECORDS ABOUT THEMSELVES**
- **ALLOWS INDIVIDUALS TO AMEND RECORDS ABOUT THEMSELVES**
- **LIMITS USE OF SSN**
- **PROVIDES JUDICIAL REMEDIES FOR PA VIOLATIONS**

SLIDE 4

FAIR INFORMATION PRACTICES

- NO SECRET SYSTEMS
- SOLICIT INFORMATION DIRECTLY FROM INDIVIDUAL
- ADVISE INDIVIDUAL OF AUTHORITY, WHETHER VOLUNTARY vs MANDATORY, PURPOSE(S), USES, EFFECTS IF INDIVIDUAL REFUSES
- CONSULT INDIVIDUAL BEFORE DISCLOSING INFORMATION OUTSIDE DOD, IF PURPOSES ARE DIFFERENT FROM ORIGINAL PURPOSE FOR COLLECTING
- GRANT ACCESS TO SUBJECT OF FILE
- ALLOW INDIVIDUAL TO REQUEST AMENDMENT TO RECORDS IN ERROR
- CHECK ACCURACY OF RECORDS BEFORE RELEASING OUTSIDE DOD

SLIDE 5

**CONDITIONS OF DISCLOSURE
AGENCY - DON**

- **GENERAL RULE: NO RECORD IN SYSTEM OF RECORDS DISCLOSED WITHOUT CONSENT OF INDIVIDUAL TO WHOM THE RECORD PERTAINS**
- **EXCEPTIONS:**
 - **NEED TO KNOW**
 - **RELEASED UNDER FOIA**
 - **ROUTINE USE**
 - **BUREAU OF CENSUS**
 - **STATISTICAL RESEARCH**
 - **NATIONAL ARCHIVES**
 - **CRIMINAL/CIVIL LAW ENFORCEMENT ACTIVITY**
 - **CIRCUMSTANCES AFFECTING HEALTH OR SAFETY OF INDIVIDUAL**
 - **COMMITTEE OF CONGRESS**
 - **COMPTROLLER GENERAL FOR GENERAL ACCOUNTING OFFICE**
 - **ORDER OF A COURT OF COMPETENT JURISDICTION**
 - **CONSUMER REPORTING AGENCY**

DISCLOSURE ACCOUNTING

**DISCLOSURE ACCOUNTINGS ARE NECESSARY
TO:**

- **TRACE DATA TO BE CORRECTED**
- **INFORM INDIVIDUALS OF DISCLOSURES
MADE**
- **MONITOR COMPLIANCE**

SECNAVINST 5211.5D
17 JUL 1992

SLIDE 8

EXCEPTIONS

DO NOT KEEP DISCLOSURE ACCOUNTING IF:

- **ACCOUNTING IS MADE BETWEEN DOD
ACTIVITIES**
- **DISCLOSED UNDER FOIA**

SLIDE 9
ACCESS TO RECORDS

ACCESS BY INDIVIDUAL:

- IN SYSTEM OF RECORDS, RETRIEVED BY INDIVIDUAL'S NAME OR OTHER PERSONAL IDENTIFIER
- ENTITLED TO ALL INFORMATION IN INDIVIDUAL'S RECORD, EVEN IF IT PERTAINS TO THIRD PARTY
- EXAMPLES OF ACCESS
- NO REASON NEEDED TO ACCESS OWN RECORDS
- THIRD PARTY TO ACCOMPANY INDIVIDUAL
- PROVIDING COPIES OF RECORDS IN COMPREHENSIBLE FORM

ACCESS TO MEDICAL RECORDS

VERIFICATION OF IDENTITY

ACKNOWLEDGEMENT OF PA REQUESTS:

- 10 BUSINESS DAYS TO ACKNOWLEDGE
- 30 BUSINESS DAYS TO RELEASE/DENY

RELATIONSHIP OF FOIA AND PA

17 JUL 1992

SLIDE 10

AMENDMENT OF RECORDS

**WITHOUT ACCESS, INDIVIDUAL HAS NO WAY OF
KNOWING WHETHER TO SEEK AMENDMENT
REQUEST FOR AMENDMENT**

- **MUST BE IN WRITING**
- **FURNISH RELEVANT EVIDENCE TO SUPPORT REQUEST**
- **AMENDMENT REQUESTS CAN ONLY BE FACTUAL, BUT
NOT JUDGMENTAL DECISIONS, e.g. FITNESS REPORTS/
RESULTS OF SELECTION OR PROMOTION BOARDS**
- **JUDGMENTAL DECISIONS TO BOARD FOR CORRECTION
OF NAVAL RECORDS**

**ACKNOWLEDGMENT OF AMENDMENT REQUEST IN 10 BUSINESS
DAYS**

DENIAL OF AMENDMENT

- **IN WRITING**
- **RIGHT TO SEEK ADMINISTRATIVE REVIEW**
- **DESCRIBE PROCEDURES FOR REQUESTING
ADMINISTRATIVE REVIEW**
- **TELL WHERE TO SEEK ASSISTANCE IN FILING
ADMINISTRATIVE APPEAL**

ADMINISTRATIVE APPEAL OF REFUSAL TO AMEND

GRANTING ADMINISTRATIVE APPEAL

DENYING ADMINISTRATIVE APPEAL

STATEMENT OF DISAGREEMENT

AGENCY STATEMENT OF AGREEMENT

JUDICIAL REVIEW

AMENDMENT PROCEDURE HELPS AGENCY:

- **ENSURE ACCURACY OF RECORDS**

SLIDE 11

AGENCY REQUIREMENTS

- **MAINTAIN ONLY RELEVANT AND NECESSARY INFORMATION**
- **COLLECT DIRECTLY FROM INDIVIDUAL**
- **INFORM INDIVIDUAL BEFORE SOLICITING INFORMATION**
- **PUBLISHING NOTICES IN FEDERAL REGISTER**
- **RECORDS MUST BE ACCURATE, RELEVANT, TIMELY AND COMPLETE**
- **MAINTAIN NO RECORDS ON FIRST AMENDMENT ACTIVITIES**
- **NOTIFICATION FOR DISCLOSURES UNDER COMPULSORY LEGAL PROCESS**
- **RULES OF CONDUCT**
- **SAFEGUARDS**

SLIDE 12

PA EXEMPTIONS

- **SUBSECTION (d)(5) - EXEMPTS INFORMATION COMPILED IN REASONABLE ANTICIPATION OF CIVIL ACTION PROCEEDING**
- **GENERAL (SUBSECTION (J))**
 - CIA
 - CRIMINAL LAW ENFORCEMENT
- **SPECIFIC (SUBSECTION (K))**
 - CLASSIFIED
 - INVESTIGATORY MATERIALS FOR LAW ENFORCEMENT PURPOSES
 - PROTECTIVE SERVICES
 - STATISTICAL RESEARCH
 - INVESTIGATORY MATERIALS FOR DETERMINING SUITABILITY, ELIGIBILITY OF QUALIFICATIONS FOR FEDERAL CIVILIAN EMPLOYMENT, MILITARY SERVICE
 - TEST OR EXAMINATION MATERIAL
 - EVALUATION MATERIAL
- **NO SYSTEM AUTOMATICALLY EXEMPT**

SLIDE 13

APPLICATION TO CONTRACTORS

- **APPLIES TO CONTRACTORS WHO ARE HIRED TO OPERATE PA SYSTEMS OF RECORDS**
- **DOES NOT APPLY TO CONSUMER REPORTING AGENCIES**
- **CONTRACT MUST SPELL OUT PA CONSIDERATIONS**
- **PROTECTIONS MUST BE IN PLACE**
- **MODIFICATIONS OF NAVAL PROCUREMENT MUST BE MADE TO PRECLUDE LIABILITY**

17 JUL 1992

SLIDE 14

PRIVACY ACT STATEMENTS

PA STATEMENT CONSISTS OF:

- STATUTE OR EXECUTIVE ORDER**
- MANDATORY vs VOLUNTARY**
- PRINCIPAL PURPOSES**
- ROUTINE USES**
- EFFECTS/CONSEQUENCES OF NOT PROVIDING INFORMATION**

PA STATEMENT MUST BE:

- IN WRITING; AND IN ONE OF THE FOLLOWING FORMATS:**
 - BODY OF THE FORM**
 - ON REVERSE SIDE OF FORM**
 - ON TEAR-OFF SHEET ATTACHED TO FORM**
 - ON SEPARATE SHEET**

17 JUL 1992

SLIDE 15

SSN's

GENERAL RULE:

**DO NOT DENY ANYONE A RIGHT, BENEFIT
OR PRIVILEGE PROVIDED BY LAW
BECAUSE INDIVIDUAL REFUSED TO
DISCLOSE HIS/HER SSN**

EXCEPTIONS:

- **DISCLOSURE OF SSN IS REQUIRED BY
FEDERAL STATUTE**
- **SYSTEM OF RECORDS WAS IN
EXISTENCE PRIOR TO JANUARY 1, 1975**

17 JUL 1992

SLIDE 16

**WHEN SOLICITING SSN's, ADVISE THE
INDIVIDUAL:**

- **WHETHER DISCLOSURE IS MANDATORY
OR VOLUNTARY**
- **UNDER WHAT STATUTE OR AUTHORITY
SSN IS SOLICITED**
- **WHAT USES WILL BE MADE OF SSN**

SLIDE 17

SYSTEMS OF RECORDS NOTICES

- **PROHIBITION AGAINST SECRET SYSTEMS OF RECORDS**
- **PUBLICATION IN FEDERAL REGISTER**
- **FORMAT/CONTENTS**

17 JUL 1992

SLIDE 18

CONFIDENTIALITY, SECURITY AND INTEGRITY OF RECORDS

- **ESTABLISH ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS TO ENSURE SECURITY AND CONFIDENTIALITY OF RECORDS**
- **SYSTEMS MANAGERS ARE RESPONSIBLE FOR IMPLEMENTING THEIR OWN POLICIES/PROCEDURES REGARDING THEIR SYSTEMS OF RECORDS**
- **DESIGNATE RECORDS CONTAINING PERSONAL INFORMATION AS "FOR OFFICIAL USE ONLY"**
- **MINIMUM REQUIREMENTS**
- **STORAGE REQUIREMENTS**
SYSTEMS MANAGERS MUST BE FAMILIAR WITH STORAGE REQUIREMENTS OF THEIR SYSTEM OF RECORDS SPECIFIED IN FEDERAL REGISTER
- **TRANSFER OF RECORDS**
- **DISPOSAL OF RECORDS**

17 JUL 1992

SLIDE 19

- **SPECIAL CONSIDERATIONS FOR PROTECTING PERSONAL INFORMATION IN AUTOMATED SYSTEMS**
- **ESTABLISHING ADP SAFEGUARDS**
 - **SENSITIVITY OF DATA**
 - **INSTALLATION ENVIRONMENT**
 - **RISK OF EXPOSURE**
 - **COST OF VARYING DEGREES OF SAFEGUARDING**
- **PHYSICAL SAFEGUARDS**
- **TECHNICAL SAFEGUARDS**
- **RISK ASSESSMENTS**
- **ESTABLISHING WORD PROCESSING SAFEGUARDS**

17 JUL 1992

SLIDE 20

CIVIL REMEDIES AND CRIMINAL PENALTIES

CIVIL REMEDIES - DON ACTIONS THAT COULD RESULT IN INDIVIDUAL FILING SUIT IN FEDERAL COURT

- REFUSAL TO GRANT ACCESS
- REFUSAL TO AMEND RECORD
- FAILURE TO MAINTAIN ACCURATE, RELEVANT,
TIMELY AND COMPLETE RECORDS
- FAILURE TO COMPLY WITH ANY OTHER PA PROVISION

- MAY BE FILED IN:

- * DISTRICT WHERE INDIVIDUAL RESIDES
- * DISTRICT WHERE RECORDS RESIDE
- * DISTRICT OF COLUMBIA

- ONLY DON CAN BE SUED; NOT EMPLOYEE OF DON
- 2 YEAR STATUTE OF LIMITATION
- REASONABLE COSTS OF LITIGATION ARE RECOVERABLE
BY ALL PA PLAINTIFFS WHO WIN

CRIMINAL PENALTIES - DON OFFICIAL OR EMPLOYEE WHO WILLFULLY:

- MAINTAINS SECRET FILES
- DISCLOSES RECORDS KNOWING IT IS VIOLATION
- REQUESTS OR OBTAINS INFORMATION UNDER FALSE
PRETENSES

- * IF FOUND GUILTY, IS CHARGED WITH MISDEMEANOR
AND FINED UP TO \$5,000.00

17 JUL 1992

**INSTRUCTIONS FOR PREPARING OPNAV FORM 5211/10,
ANNUAL REPORT - PRIVACY ACT****BACKGROUND:**

The Privacy Act Report is mandated by statute. It is designed to provide Congress with the information describing the exercise of individual rights of access and amendment, identifying changes in or additions to systems of records, and describing certain administrative actions that would be useful to Congress in reviewing the effectiveness of the PA program.

RESPONSIBILITY:

Echelon 2 commands are responsible for collecting and consolidating reports from each subordinate command (i.e., Commander, Naval Facilities Engineering Command will consolidate reports for the Western Division, Pacific Division, etc., and CMC (Code MI-3) will consolidate reports for all Marine Corps activities and provide CNO (OP-09B30) with a consolidated report by 30 March of each year.

Echelon 2 commands and CMC shall forward their consolidated reports to CNO (OP-09B30) for compilation and submission to the Office of the Secretary of Defense (Director, Administration and Management) (OSD (DA&M)). Please ensure that your report contains your complete address, telephone number, and point of contact, should questions arise.

All other activities shall include the same identifying data in their report submission.

Should you require assistance in preparing the report, please feel free to contact CNO (OP-09B30), DSN 224-2004/2817, or Commercial (703) 614-2004/2817, for assistance.

REPORT CONTROL SYMBOL: DD-DA&M(AR)1379

NEGATIVE REPORTS: If any DON activity has not received a PA request during the reporting period, place an "X" in the box marked "negative reports" and submit your report through the next chain of command. Ships and operational aviation squadrons that have not received any requests during the reporting period are exempt from reporting.

CONTENTS OF REPORT:

SECTION A: Complete this section if you received PA

Enclosure (16)

SECNAVINST 5211.5D

17 JUL 1992

requests during the reporting period.

SECTION B: Only ASN (M&RA), NJAG, and OGC complete this section and forward to CNO (OP-09B30).

SECTION C: Only CNO (OP-09B30) and CMC (MI-3) complete this section.

PRIVACY ACT REPORT
(DD-DA&M(AR) 1379)

FROM:

Activity

POC (name & rank)

Phone

CHECK HERE FOR NEGATIVE REPORT

SECTION A: (To be completed by all naval activities that received/responded to a PA request during the reporting period.)

- | | |
|---|----------------------|
| 1. Number of requests received for access | <input type="text"/> |
| 2. Number of access requests completely or partially granted | <input type="text"/> |
| 3. Number of access requests denied in whole | <input type="text"/> |
| 4. Number of access requests for which no record was found | <input type="text"/> |
| 5. Number of requests to amend records | <input type="text"/> |
| 6. Number of amendment requests completely or partially granted | <input type="text"/> |
| 7. Number of amendment requests denied in whole | <input type="text"/> |
| 8. Number of amendment requests in which no record was found | <input type="text"/> |

SECTION B: (To be completed by ASN(M&RA/OGC/NJAG only.)

- | | |
|--|----------------------|
| 1. Number of appeals from denials of access | <input type="text"/> |
| 2. Number of appeals from denials of access in which denial was upheld | <input type="text"/> |
| 3. Number of appeals from denials of access in which the denial was overturned completely or partially | <input type="text"/> |
| 4. Number of appeals from denials of amendments | <input type="text"/> |
| 5. Number of appeals from denials of amendments in which the denial was upheld | <input type="text"/> |
| 6. Number of appeals from denials of amendments in which the denial was overturned completely or partially | <input type="text"/> |
| 7. Number of instances in which individuals litigated the results of appeals from denials of access or amendment | <input type="text"/> |
| 8. Synopsise all PA litigation that was filed or completed during the calendar year. | |

SECTION C: (To be completed by CNO (OP-09B30) and CMC (MI-3) only.)

	Exempt	Non-Exempt
1. Total number of active systems	<input type="text"/>	<input type="text"/>
2. Number of new systems established during the year	<input type="text"/>	<input type="text"/>
3. Number of systems deleted during the year	<input type="text"/>	<input type="text"/>
4. Number of systems automated, either in whole or in part, during the year	<input type="text"/>	<input type="text"/>
5. Number of existing systems for which new routine uses were established during the year	<input type="text"/>	<input type="text"/>
6. Number of existing systems of records for which new exemptions were established during the year	<input type="text"/>	
7. Number of existing systems for which exemptions were deleted during the year	<input type="text"/>	
8. Number of matching programs during the year	<input type="text"/>	
9. Number of matching programs in which DON was the source agency	<input type="text"/>	
10. Number of hits resulting from the matching programs	<input type="text"/>	
11. Description of any recovery actions taken as a result of the matching programs.		
12. Summary of training programs conducted during the calendar year.		

17 JUL 1992

SAMPLE CHECKLIST FOR CONDUCTING PA STAFF ASSISTANCE VISITS**1. MANAGEMENT**

a. Has the head of the activity designated a PA coordinator to serve as the principal point of contact on privacy matters and be responsible for effective implementation and compliance? Is this designation in writing? Are these duties reflected in his/her job description?

b. Has an effective PA program been established and maintained through all echelons, with adequate funding and sufficient experienced staff at all levels, designated to ensure effective compliance? Is there a listing of the PA points of contacts at the lower echelons?

c. Is the designated PA coordinator responsible within his/her jurisdiction for monitoring, inspecting and reporting on the status of the activity's PA program at all echelons? Has there been a recent review of one of those activities? If so, is there a report of findings?

d. Are responsible PA coordinators at various echelons adequately staffed and trained to accomplish their responsibilities?

e. Has the command adequately implemented SECNAVINST 5211.5D by publishing internal command procedural rules?

2. ADMINISTRATION, TRAINING, AND COMPLIANCE MONITORING

a. Are all command echelons knowledgeable of the rules of conduct for persons involved in the design, development, operation or maintenance of any system of records? Is there a listing of those systems of records that are maintained and a listing of the systems managers responsible for maintaining those systems?

b. What training has the PA coordinator received? What orientation training have command personnel received concerning their rights and responsibilities under the PA? What training have systems managers, denial authorities, and senior management personnel received who are responsible for systems of records? What training have specialized personnel (i.e., financial, medical, law enforcement, records management) received who are responsible for processing personal information on a daily basis? How often are these individuals being trained? Has the PA film

Enclosure (17)

17 JUL 1992

been shown to all personnel?

c. Are there established activity procedures in place to ensure effective compliance under section (m) of the Act by contractors?

d. What guidance is the naval activity following to determine how long PA records are to be maintained?

e. Where is the PA program located? Is this the most feasible place? Is legal support available?

3. INFORMATION MANAGEMENT REQUIREMENTS

a. Does the activity only maintain information about an individual that is relevant, timely, necessary, and complete to accomplish a purpose of the activity required by statute or by E.O.?

b. Is the information collected, to the greatest extent practicable, directly from the individual when the information may result in adverse determinations about an individual's right, benefit, and privileges under Federal programs?

c. Is the individual advised that E.O. 9397 is the authority for requesting his/her SSN? When requesting other personal information from an individual, is he/she informed through a Privacy Act Statement (PAS), the authority for requesting the information, the purposes for which the information was collected, the routine uses/users for the information, and whether providing the information is voluntary or mandatory and the consequences for not disclosing it? Are any rights, benefits, or privileges being denied because the individual refuses to disclose his/her SSN or other items of personal information being requested? Ask for sample PAS's currently being used.

d. Are appropriate administrative, technical, and physical safeguards established to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is being maintained? Are the guidelines for using and safeguarding records in computerized data bases and in word processors, as addressed in this instruction, being implemented?

Enclosure (17)

17 JUL 1992

4. SYSTEMS OF RECORDS

a. Does the PA coordinator have copies or records of the identification and location of each recordkeeping function subject to the PA and the corresponding PA systems notice for his/her command? Has the PA coordinator disseminated a listing of each system of records being maintained and who is the systems manager for each?

b. Are procedures/reviews in place to ensure that no recordkeeping function retrievable by a personal identifier is being operated without first being reported and published in the Federal Register? Does the PA coordinator know where to seek assistance when an unreported system of records has surfaced?

c. In actual practice, are the routine uses made of records from systems of records in conformity with the listed routine use element of the published notice?

d. Are the routine uses in the notice compatible with the purpose for which the record was collected?

e. Compare the elements of the published systems notice with the actual practices/procedures in effect. Do they conform?

5. FORMS

a. Are PAS's given for all forms, questionnaires, survey sheets, reports, etc., which solicit personal information directly from the individual? Ask to see samples of PAS's for review.

b. Does the PAS on the form meet the requirements of paragraph 10d of SECNAVINST 5211.5D?

6. ACCESS

a. Are requests for access acknowledged within the 10 working day time limit? Ask to see samples of acknowledgement letters and the way of tracking these requests.

b. Is access provided to the individual within 30 working days?

7. AMENDMENTS TO RECORDS

a. Are amendment requests acknowledged within 10 working days and accomplished within 30 days of receipt?

Enclosure (17)

17 JUL 1992

b. Are previous recipients of the records notified when a requested amendment is honored?

c. Does the activity's denial authority make a review of the refusal within 30 working days after receipt of the individual's appeal? If the individual is refused, is the required information provided to him/her?

d. Have records been annotated to reflect the designated portions indicated in the individual's statement of dispute? Where an accounting of disclosure has been made, have the previous recipients of the record been provided a copy of the individual's statement? Ask to see examples of this process for review.

8. DISCLOSURE

a. Are disclosures of personal information made as prescribed by paragraph 13 of SECNAVINST 5211.5D?

b. Are accurate disclosure accountings of all disclosures made from an individual's record being maintained? Are they being retained for five years or the life of the record, whichever is longer? Ask to see a sampling of disclosure accounting sheets for review.

9. REPORT

a. What procedures have been set up to collect PA statistics?

b. Is the most current format being used?

c. What guidance is provided to subordinate activities for compiling the PA report statistics?

d. Does the PA coordinator maintain a list of subordinate points of contacts and their addresses of those who submit PA reports?

17 JUL 1992

COMPUTER MATCHING GUIDELINES

1. GENERAL

a. Scope. The PA and this instruction are applicable to certain types of computer matching--the computer comparison of automated systems of records.

b. Compliance. Although the PA provides for specific procedures, it is not in itself authority for carrying out any matching activity. Compliance with this enclosure does not relieve a DON activity of the obligation to comply with any other requirements of the PA and this instruction.

c. Matching programs covered by the PA. There are two specific kinds of matching programs that are fully governed by the PA and this instruction. These are:

(1) Matches using records from Federal personnel or payroll systems of records as described under Definitions.

(2) Matches involving Federal benefit programs to accomplish one or more of the following purposes:

(a) To determine eligibility for a Federal benefit.

(b) To comply with benefit program requirements.

(c) To effect recovery of improper payments or delinquent debts from current or former beneficiaries.

d. Automated comparisons. The record comparison must be a computerized comparison, manual comparisons are not covered, involving records from:

(1) Two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to the PA); or,

(2) A DON activity's automated system of records and automated records maintained by a non-Federal agency (i.e., state or local government or agent thereof).

e. Features of a matching program. A covered computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the Federal

17 JUL 1992

Register before the match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any.

2. FEDERAL PERSONNEL OR PAYROLL RECORDS MATCHES

a. Scope. These computer matching programs include matches comparing records from DON automated Federal personnel or payroll systems of records with similar automated records of another Federal agency; or with a non-Federal agency. It also includes matches between DoD Components or within the DON activity itself (internal matches).

b. Computerized comparison. The matching must be done using a computer. Manual comparisons are not covered.

c. Exclusion. Matches must be done for other than "routine administrative purposes", as explained in paragraph 4f.

d. Internal matches. In some instances, a covered match may take place within a DON activity or with another DOD Component. For example, a DON activity may wish to determine whether any of its own personnel, participating in a benefit program administered by the DOD, are not complying with the program's eligibility requirements. This internal match will certainly result in an adverse action if ineligibility is discovered. Therefore, it is covered by the requirements of the PA. DON activities should not attempt to avoid the reach of the Act, for example, by improperly combining dissimilar systems into a single system, matching data within that system to make an eligibility determination, and arguing that the match is not covered because only one system of records is involved.

e. Categories of record subjects. The categories of individuals whose records are used in this type of matching program must be carefully analyzed before making a determination whether a proposed match is covered. All information on record subjects is maintained in DON's system of records, but matching under the particular programs covered by this paragraph is limited to "Federal personnel." For example, a DON activity's automated record system containing a voluntary survey of high school seniors' attitude toward military service is requested by the Selective Service System to be matched for the purpose of policing draft registration compliance. This particular match would not be covered by the Act or this Instruction and could not proceed because the high school seniors do not meet the definition of "Federal personnel" even though the information is maintained in a PA system of records. As a practical matter, the DON activity could still refuse to participate in the match on

the basis that the needed routine use disclosure to the Selective Service System would not meet the compatibility test. For matching purposes a Federal personnel system of records should not be confused with, or limited to, the commonly recognized personnel system of records maintained by a civilian personnel office or a military assignment branch. A DON activity may be maintaining within a single system of records several categories of records relating to Federal personnel and other categories on non-Federal personnel, e.g., contractor personnel, applicants, dependents, etc. Some categories may be covered while others may not be covered. Unlike "Federal personnel", the record subjects of payroll record systems are easily discerned.

f. Matching purpose. The purpose of a Federal personnel or payroll records match must be to take some adverse action, i.e., financial, personnel, disciplinary, or other adverse action against Federal personnel.

3. FEDERAL BENEFIT MATCHES

a. Categories of subjects covered. The PA provisions cover only the following categories of record subjects for Federal benefit matches.

(1) Applicants for Federal benefit programs (i.e., individuals initially applying for benefits);

(2) Program beneficiaries (i.e., individuals currently receiving or formerly receiving benefits);

(3) Providers of services to support such programs (i.e., those deriving income from them such as health care providers).

b. Types of programs covered. Only Federal benefit programs providing cash or in-kind assistance to individuals are covered by the PA. State programs are not covered. Programs using records about subjects who are not "individuals" as defined under definitions are not covered.

c. Matching purpose. A Federal benefit match must have as its purpose one or more of the following:

(1) Establishing or verifying initial or continuing eligibility for Federal benefit programs.

(2) Verifying compliance with the requirements, either statutory or regulatory, of such programs.

17 JUL 1992

(3) Recouping payments or delinquent debts under such Federal benefit programs.

d. Summary of basic requirements. Four basic elements--computerized comparison, categories of subjects, Federal benefit program, and matching purpose--must all be present before a matching program is covered under the PA.

4. MATCHING PROGRAM EXCLUSIONS

The following are not included under the definition of a matching program. DON activities operating such programs are not required to comply with the computer matching provisions of the PA, although they may be required to comply with any other applicable provisions of the Act and this instruction.

a. Statistical matches whose purpose is solely to produce aggregate data stripped of personal identifiers. This does not mean that the data bases used in the match must be stripped prior to the match, but only that the results of the match must not contain data identifying any individual. Implicit in this exception is that this kind of match is not done to take action against specific individuals.

b. Statistical matches whose purpose is in support of any research or statistical project. The results of these matches need not be stripped of identifiers, but they must not be used to make decisions that affect the rights, benefits or privileges of specific individuals.

c. Pilot matches. This exclusion covers small scale sampling matches whose purpose is to gather cost-benefit data on which to premise a decision about engaging in a full-fledged matching program. Pilot matches must be retained in a statistical information gathering channel. It is at this point that the DON activity can decide whether to conduct a statistical data gathering match without consequences to the record subjects or a full-fledged program where results will be used to take specific action against them. To avoid possible misuse of pilot matches and to ensure full compliance with the PA, these matches must be approved by the Defense Data Integrity Board.

d. Law enforcement investigative matches whose purpose is to gather evidence against a named person or persons in an existing investigation.

(1) To be eligible for the exclusion the match must

be performed by an activity of a component whose principal function involves enforcement of criminal laws, i.e., an activity that is authorized to exempt certain of its systems of records under subsection (j)(2) of the PA.

(2) The match must flow from an investigation already underway which focuses on a named person or persons. Fishing expeditions are not eligible for this exclusion. Subjects identified generically, e.g., "program beneficiaries", are not eligible.

(3) The investigation may be into either criminal or civil law violations.

(4) In the context of this exclusion only, person or persons could include subjects that are other than individuals as defined in the PA, such as corporations or other business entities. For example, a business entity could be named subject of the investigation and records matched could be those of customers or clients.

(5) The match must be for the purpose of gathering evidence against the named person or persons.

e. Tax administration matches.

(1) Matches involving disclosures of taxpayer return information to State or local tax officials under section 6103(d) of the Internal Revenue Code.

(2) Tax refund offset matches accomplished under the Deficit Reduction Act of 1984.

(3) Matches done for tax administration under section 6103(b)(4) of the Internal Revenue Code.

(4) Tax refund offset matches conducted under other statutes provided approval of the Office of Management and Budget is obtained.

f. Routine administrative matches using Federal personnel records. These are matches between a DON activity and other Federal agencies or between a DON activity and non-Federal agencies for administrative purposes that use data bases that contain records predominantly relating to Federal personnel. The term "predominantly" means that the percentage of records in the system that are about Federal employees must be greater than of any other category contained there. For the purpose of

SECNAVINST 5211.5D

17 JUL 1992

disclosing records subject to the PA, the DOD is considered a single agency.

(1) The purpose of the match must not be intended to result in an adverse action. Matches whose purpose is to take any adverse financial, personnel, disciplinary or other adverse action against Federal personnel whose records are involved in the match, are not excluded from the Act's coverage.

(2) Examples of matches that are excluded are an agency's disclosure of time and attendance information on all agency employees to the Department of the Treasury in order to prepare the agency's payroll; or disclosure of DON reserve officer identifying information to a state in order to validate and update addresses of reservists residing in the state; and disclosure of retiree annuity files from the DON to the Department of Veterans Affairs (VA) in order to determine the percentage of total annuity each agency is responsible for paying.

(3) This exclusion does not bring under the Act's coverage matches that may ultimately result in an adverse action. It only requires that their purpose not be intended to result in an adverse action. In the DON/state reservist match example, the ultimate consequence of the match may well be that a reservist is dropped from the program because no address can be found. This result, however negative, would not bring the match under the Act's coverage since its primary purpose was only to update an address listing.

g. Internal matches using only records from DOD systems of records.

(1) Internal matches (conducted within the DOD) is excluded on the same basis as Federal personnel record matching above (see paragraph 2b) provided no adverse intent as to a Federal employee motivates the match.

(2) This exclusionary provision does not disturb subsection (b)(1) of the Act permitting disclosure to DOD employees on an official need-to-know basis. For example, the Navy could match with the Office of the Assistant Secretary of Defense (Force Management & Personnel) for an accounting reconciliation to locate individuals. The Defense Logistics Agency could match, using its automated systems of records, to determine the specific health insurance plan associated for each member. The Defense Finance and Accounting Service (DFAS) could

17 JUL 1992

match with the Deputy Commander for Operations, Flight Records Branch (DOTF) to determine who is eligible to receive flight pay, but if DFAS would consider a match for the purpose of recouping flight pay paid to those that were ineligible to receive it, then the match would be covered because of the adverse purpose of the match.

(3) The purpose of the internal match must not be to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel.

k. Background investigation and foreign counterintelligence matches. Matches done in the course of performing a background check for security clearances of Federal personnel or Federal contractor personnel are not covered. Matches done for the purpose of foreign counterintelligence are also not covered.

5. CONDUCTING MATCHING PROGRAMS

a. Source and recipient agencies. A DON activity undertaking a matching program should consider if it will be a "source agency" or a "recipient agency" for the match (see Definitions) and be prepared to meet the following requirements:

(1) The recipient agency does the matching. It receives the data from system of records of other Federal agencies or data from state and local governments and actually performs the match by computer.

(2) The recipient agency is responsible for publishing a notice in the Federal Register of the matching program as required in paragraph 5d of this enclosure. Where a state or local agency is the recipient, the Federal source agency is responsible for publishing the notice.

(3) A Federal source agency discloses the data from a system of records for the match. A non-Federal agency may also be a source, but the record data will not be from a system of records. The "system of records" concept under the PA does not apply to the recordkeeping practices of state or local governmental agencies.

(4) The recipient Federal agency, or the Federal source agency in a match performed by a non-Federal agency, is responsible for reporting the match. This agency must contact the other participants to gather the information necessary to make a unified report as required by paragraph 12 of this enclosure.

17 JUL 1992

(5) In some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match; or when as a practical matter, an agency may not wish to release and disclose its data base to another agency as a source because of privacy safeguard considerations. For example, if the parent locator service of a state wishes to conduct a match with a DON activity to locate 300 missing parents, it would be impractical for the DON activity to provide its entire data base consisting of over six million record subjects to the state as a source agency, but it may be willing to entertain a request for the match as a recipient agency.

b. Compliance with the system of records and disclosure provisions.

(1) The DON activity must ensure that it identifies the system(s) of records involved in the matching program and has published the necessary notice(s) in the Federal Register.

(2) The PA does not itself authorize disclosures from system of records for the purpose of conducting a matching program. A DON activity must justify any disclosures outside the DOD under subsection (b) of the Act. This means obtaining the written consent of the record subjects for the disclosure or relying on one of the 12 nonconsensual disclosures exceptions to the written consent rule. To rely on the routine use exception (b)(3), the DON activity must have already established the routine use (published in the Federal Register), or in the alternative, must comply with subsections (e)(4)(d) and (e)(11) of the Act which means amending the record system notice to add an appropriate routine use for the match. An amendment requires publication in the Federal Register with a 30 day waiting period for public comment.

(3) The routine use permitting disclosure for the match must be compatible with and related to the purpose for which the record was initially compiled.

(4) The routine use for the match in a record system notice shall clearly indicate that it entails a computer matching program with a specific agency for an established purpose and intended objective. For purposes of matching, a routine use must state that a disclosure may be made for a matching program. DON activities may not rely on an existing established routine use to meet the requirements of the Act unless it expressly permits disclosure for matching purposes.

17 JUL 1992

c. Prior notice to record subjects. Record subjects must receive prior notice that their records may be matched. This may be done by direct and/or constructive notice.

(1) Direct notice may be given when there is some form of contact between the government and the subject. Information can be furnished to individuals on the application form when they apply for a benefit, in a notice that arrives with a benefit, or in correspondence they receive in the mail. Use of the PAS is an acceptable manner to provide direct notice to record subjects at the time of application. DON activities shall provide direct notice for front-end eligibility verification matching programs whose purpose is to validate an applicant's initial eligibility for a benefit and later to determine continued eligibility using the PAS on the application form. Providers of services should be given notice on the form on which they apply for reimbursement for services provided. Providing notice of matching programs using the PAS shall be part of the normal process of implementing a Federal benefits program. DON activities shall insure records contain appropriate revisions.

(2) Constructive notice can only be given by an appropriate routine use disclosure provision of the affected system of records to be used in the match. For purely internal matching program uses, amend the "Purpose(s)" element of the record system notice to specifically reflect those internal computer matches performed. The constructive notice method requires publication in the Federal Register. Examples of when constructive notice may be used are:

(a) For matching programs whose purpose is to locate individuals in order to recoup payments improperly granted to former beneficiaries, direct notice may well be impossible and constructive notice may have to suffice.

(b) A DON activity that discloses records to a state or local government in support of a non-Federal matching program is not obligated to provide direct notice to each record subject. Federal Register publication in this instance is sufficient.

(c) Investigative matches where direct notice immediately prior to a match would provide the subject an opportunity to alter behavior.

(3) DON activities shall also provide periodic notice whenever an application is renewed, or at the least during the period the match is authorized to take place by providing notice accompanying the benefit as approved by the Defense

17 JUL 1992

Data Integrity Board.

d. Publication of the matching notice

(1) The matching agency is required to publish in the Federal Register a notice of any proposed matching program or alteration of an established program at least 30 days prior to conducting the match for any public comment. Only one notice is required. When a non-Federal agency is the matching agency, the DON activity source agency shall be responsible for the publication. The proposed matching notice for publication shall be submitted in Federal Register format and included in the DON activity's report of a proposed match. The notice shall contain the customary preamble and contain the required information in sufficient detail describing the match so that the reader will easily understand the nature and purpose of the match, including any adverse consequences.

(2) The preamble to the notice shall be prepared by the Defense Privacy Office and shall contain:

(a) The date the transmittal letters to OMB and Congress are signed.

(b) A statement that the matching program is subject to review by OMB and Congress and shall not become effective until that review period has elapsed.

(c) A statement that a copy of the agreement shall be available upon request to the public.

(3) The DON activity shall provide:

(1) Name of participating activity.

(2) Identity of the source agency and the recipient agency, or in the case of an internal DoD matching, the DON activities involved.

(3) Purpose of the match being conducted to include a description of the matching program and whether the program is a one-time or a continuing program.

(4) Legal authority for conducting the matching program. Do not cite the PA as it provides no independent authority for carrying out any matching activity. If at all possible, use the U.S. Code citations rather than the public law as access to the Public Laws is more difficult. Avoid citing

17 JUL 1992

housekeeping statutes such as 5 U.S.C. 301, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information even if it results in citing the Code of Federal Regulations or a DoD directive or regulation. Whenever possible, the popular name or subject of the authority should be given, as well as a statute, public law, U.S. Code, or Executive Order number; for examples: The Debt Collection Act of 1982 (Pub. L. 97-365) 5 U.S.C. 5514, Installment Deduction of Indebtedness; and 4 CFR Chapter II, Federal Claims Collection Standards (General Accounting Office-Department of Justice).

(5) A complete description of the system(s) of records that will be used in the match. Include the system identification, name, and the official Federal Register citation, date published, including any published amendments thereto. Provide a positive statement that the system(s) contains an appropriate routine use provision authorizing the disclosure of the records for the purpose of conducting the computer matching program. (Note: In the case of internal DoD matches, the "purpose(s)" element of the system(s) involved.) If non-Federal records are involved, a complete description to include the specific source, address, and category of records to be used, e.g., Human Resources Administration Medicaid File, City of New York, Human Resources Administration, 250 Church Street, New York, NY 10013.

(6) A complete description of the category of records and individuals covered from the record system(s) to be used, the specific data elements to be matched, and the approximate number of records that will be matched.

(7) The projected start and ending dates for a one-time match or the inclusive dates for a continuing match.

(8) The address for receipt of any public comment or inquiries concerning the notice shall indicate: Director, Defense Privacy Office, 400 Army Navy Drive, Room 205, Arlington, VA 22202-2884.

6. PROVIDING DUE PROCESS TO MATCHING SUBJECTS

a. Independent verification and notice. Record subjects of matching programs shall be afforded certain due process procedures when a match uncovers any disqualifying or adverse information about them. No recipient agency, non-Federal agency, or source agency shall take any adverse action against an individual until such agency has independently verified such information and the individual has received a notice from the

17 JUL 1992

agency containing a statement of its findings and gives the individual the opportunity to contest the findings before making a final determination. DON activities shall not take any adverse action based on the raw results of a computer matching program. Adverse information developed by a match must be investigated and verified prior to any action being taken.

b. Independent investigation. Conservation of resources dictates that the procedures for affording due process be flexible and suited to the data being verified and the consequences to the individual of making a mistake. If the source agency has established a high degree of confidence in the quality of its data and it can demonstrate that its quality control processes are rigorous, the recipient agency may choose to expend fewer resources in independently verifying the data. Absolute confirmation is not required. DON activities should bring some degree of reasonableness to the process of verifying data. Some methods to consider are:

(1) Contact the individual record subject who is the best source where practical. In some cases, contacting the subject initially may permit the individual to conceal data relevant to a decision.

(2) Research of source documents.

c. Notice and opportunity to contest. DON activities are required to notify matching subjects of adverse information uncovered during a matching program and give them an opportunity to contest and explain before the agency makes a final determination. Recipients already receiving benefits may not have them suspended or reduced pending expiration of the contest period. Individuals have 30 days to respond to a notice of adverse action, unless a statute or regulation grants a longer period. The period runs from the date of the notice until 30 calendar days. DON activities shall allow an additional 5 days for mailing time before ending the notice period. If an individual contacts the DON activities within the notice period (35 days) and indicates his/her acceptance of the validity of the adverse information, the DON activity may take immediate action to deny or terminate. However, DON activities are cautioned against attempting to coerce a record subject into accepting the result. DON activities may also take action if the period expires without a response.

d. Combining verification and notice requirements. It may be appropriate to combine the verification and notice requirements into a single step, especially if the record subject

is the best source for verification. In this manner, the adverse finding and notice of the opportunity to contest are compressed into a single action. This method is dependent upon the confidence, reliability and quality of the data, as set forth in paragraph b above. Careful thought should be given as to when to apply this method. It may be applicable in special cases, but should not be considered as a routine process. To ensure that this consideration take place, it shall be the responsibility of the Defense Data Integrity Board to make a formal determination as to when it is appropriate to compress the verification and notice into a single period.

e. Individual status pending due process. DON activities may not make a final determination as to applicants for Federal benefit programs whose eligibility is being verified through a matching program until they have completed the due process steps the Act requires. This does not require placing an applicant on the rolls pending a determination, but only that the agency not make a final determination. However, if a subject is already receiving benefits, the benefits shall not be suspended or reduced until due process steps have been completed. If the specific Federal benefit program involved in the match has its own due process requirements, those requirements may suffice for the purposes of the PA, provided the Defense Data Integrity Board determines that they are at least as strong as the PA provisions.

f. Exclusion

(1) If a DON activity determines a potentially significant effect on public health or safety is likely, it may take appropriate action, notwithstanding these due process requirements.

(2) In such cases, the DON activity shall include the possibility of suspension of due process for this reason in its matching program agreement.

7. MATCHING PROGRAM AGREEMENT

a. Requirements. A DON activity should allow sufficient lead time to ensure that a matching agreement between the participants can be negotiated and signed in time to secure the Defense Data Integrity Board decision before the match begins. A DON activity receiving records from or disclosing records to a non-Federal agency for use in a matching program is responsible for preparing the matching agreement and should solicit relevant data from the non-Federal agency where necessary. Both Federal source and recipient agencies must have

17 JUL 1992

the matching agreement approved by their respective Data Integrity Boards. In cases where matching takes place entirely within the DON, the DON activity may satisfy the matching agreement requirements by preparing a Memorandum of Understanding (MOU) between the systems of records managers involved. Before a DON activity may participate in a matching program the Defense Data Integrity Board must have evaluated the proposed match and approved the terms of the matching agreement or MOU in accordance with paragraph 10 of this enclosure. Agreements or MOUs must contain the following elements:

(1) Purpose and legal authority. Citation of the Federal or state statutory or regulatory authority for undertaking the matching program. Do not cite the PA.

(2) Justification and expected results. A full explanation of why a computer matching program, as opposed to some other form of activity, is being proposed and what the expected results will be, including a specific estimate of any savings.

(3) Records description. A full identification of the system of records (Federal Register citations) or non-Federal records, number of record subjects, and what data elements will be included in the match.

(4) Dates. An indication of whether the match is a one-time or continuing program (not to exceed 18 months) and the projected starting and completion dates for the match.

(5) Prior notice to record subjects. A description of the direct and constructive notice procedures afforded the record subjects. Provide copies of the published applicable record system notices involved and all applicable forms containing the appropriate PAS being used by the participants of the proposed match.

(6) Verification procedures. A full description of the methods the DON activity will use to independently verify the information obtained through the matching program.

(7) Disposition of matched items. A statement that the information generated as a result of the matching program will be destroyed as soon as it has served the matching program's purpose and any legal retention requirements the DON activity establishes in conjunction with the National Archives and Records Administration or other cognizant authority.

17 JUL 1992

(8) Security procedures. A description of the administrative, technical and physical safeguards to be used in protecting the information. They should be commensurate with the level of sensitivity of the data.

(9) Records usage, duplication and redisclosure restrictions. A description of any specific restrictions imposed by either the source agency or by statute or regulation on collateral uses of the records used in the matching program. Recipient agencies may not use the records obtained for a matching program under a matching agreement for any other purpose unless there is a specific statutory authority or there is a direct essential connection to the conduct of the matching program. Agreements shall specify how long the recipient agency may keep records provided for a matching program and when they will be returned to the source agency or destroyed.

(10) Records accuracy assessments. A description of any information relating to the quality of the records to be used in the matching program such as the error rate percentage of the data entry for the affected records. The worse the quality of the data, the less likely the matching program will have a cost-beneficial result.

(11) Disclosure accounting. A certification by a DON activity participating in a matching program as a source agency for disclosures outside the DOD that a disclosure accounting shall be maintained on the record subjects as required by the PA.

(12) Access by the Comptroller General. A statement that the Comptroller General may have access to all records of a recipient DON activity or non-Federal agency necessary to monitor or verify compliance with the agreement. In this instance, the Comptroller General may inspect state or local government records used in matching programs.

b. Non-Federal agencies. Non-Federal agencies intending to participate in covered matching programs are required to do the following:

(1) Execute matching agreements prepared by a Federal agency or agencies involved in the matching program.

(2) Provide data to Federal agencies on the costs and benefits of matching programs.

(3) Certify that they will not take adverse action

17 JUL 1992

against an individual as a result of any information developed in a matching program unless the information has been independently verified and until the applicable number of days after the individual has been notified of the findings and given an opportunity to contest them has elapsed.

(4) For renewals of matching programs, certify that the terms of the agreement have been followed.

c. Duration of matching programs. Matching agreements will remain in force only as long as necessary to fulfill their specific purposes. They will automatically expire 18 months after their approval unless the Defense Data Integrity Board grants an extension of up to 1 year at least 3 months prior to the actual expiration date. The program must remain unchanged if an extension is to be granted. Each party to the agreement must certify that the program has been conducted in compliance with the matching agreement. Requests for extensions shall be submitted through channels to the Board in accordance with paragraph 12c(3) of this enclosure.

d. Altered matching program

(1) An altered matching program is one that is already established, but with such a significant change proposed that it requires revision of the matching notice and approval of the Defense Data Integrity Board, OMB and Congress. A significant change is one which does one or more of the following:

(a) Changes the purpose for which the program was established.

(b) Changes the matching population either by including new categories of record subjects, or by greatly increasing the numbers of records matched.

(c) Changes the legal authority under which the match was being conducted.

(d) Changes the records (data elements) that will be used in the match.

(2) A proposal to alter an established matching program shall be submitted through channels to the Defense Data Integrity Board for review and approval in accordance with paragraph 12c(2) of this enclosure.

e. Noncompliance sanctions

(1) No DON activity shall disclose any record for use in a matching program as a source agency to any recipient agency (within or outside the DOD) if there is reason to believe that the terms of the matching agreement/MOU or the due process requirements are not being met by the recipient agency. Inform the Defense Privacy Office immediately, through channels, should any such incident occur. See also paragraph 9c of this enclosure. Normally consulting with the recipient agency should resolve the problem, but the responsibility rests with the DON source.

(2) No DON source agency shall renew a matching agreement/MOU unless the recipient agency (within or outside the DOD) has certified that it has complied with the provisions of the agreement/MOU and the DON activity has no reason to believe otherwise.

(3) A willful disclosure of records from a system of records for any unauthorized computer matching program may subject the responsible officer or employee to criminal penalties. Civil remedies are also available to matching program subjects who can show they were harmed by an agency's violation of the Act, this Instruction or its own.

8. COST-BENEFIT ANALYSIS

a. Purpose of requirement. The requirement for a cost-benefit analysis by the Act is to assist the agency in determining whether or not to conduct or participate in a matching program. Its application is required in two places: (1) as an agency conclusion in the matching agreement containing the justification and specific estimate of savings; and (2) in the Defense Data Integrity Board review process where it is forwarded as part of the matching proposal. The intent of this requirement is not to create a presumption that when agencies balance individual rights and cost savings, the latter should inevitably prevail. Rather, it is to ensure that sound management practices are followed when agencies use records from PA systems in matching programs. It is not in the government's interest to engage in matching activities that drain agency resources that could be better spent elsewhere. Agencies should use the cost-benefit requirement as an opportunity to re-examine programs and weed out those that produce only marginal results.

b. Cost-benefit analysis. DON activities proposing matching

17 JUL 1992

programs must provide the Board with all information which is relevant and necessary to allow the Board to make an informed decision including a cost-benefit analysis. The Defense Data Integrity Board shall not approve any matching agreement unless the Board finds the cost-benefit analysis demonstrates the program is likely to be cost effective. All decisions of the Board will be well-documented.

(1) The Board may waive the cost-benefit analysis requirement if it determines in writing that submission of such an analysis is not required.

(2) If a matching program is required by a specific statute, a cost-benefit analysis is not required. However, any renegotiation of such a matching agreement shall be accompanied by a cost-benefit analysis. The finding need not be favorable. The intent, in this case, is to provide Congress with information to help it evaluate the effectiveness of statutory matching requirements.

(3) The Board must find that agreements conform to the provisions of the Act and appropriate guidelines, regulations, and statutes.

9. DEFENSE PRIVACY OFFICE

a. General. The Defense Privacy Office, ODA&M (OSD), established by reference (b), serves as the DOD focal point for policy, procedures and practices on all matters pertaining to the PA in coordination with the:

- (1) Defense Data Integrity Board.
- (2) Defense Privacy Board.
- (3) Defense Privacy Board Legal Committee.
- (4) Office of Management and Budget.
- (5) General Accounting Office.
- (6) Office of the Federal Register, in conjunction with the OSD Federal Register Liaison Officer.
- (7) DOD Components.
- (8) Other Federal agencies.

17 JUL 1992

b. **Responsibilities.** The Office consists of a Director, who also functions as the Executive Secretary on both the Defense Data Integrity Board and the Defense Privacy Board, and a staff. The Director and staff are responsible for the implementation of the PA within the DOD through this instruction by the DOD PA program and for administratively supporting both Boards and Legal Committee, set forth in paragraph 9a.

c. **Information maintenance and dissemination.** The Office is an information resource on the Privacy Act and its implementation within the DOD. While the two Boards and Committee convene only periodically at the call of the Executive Secretary, the Office serves as the full-time designated focal point for the DOD PA Program and its implementation, to provide guidance and answers on the PA from within the DOD and from outside entities. This point of contact shall be able to advise on what actions are needed to comply with the matching provisions of the PA and to receive complaints for appropriate action on any allegation or report of non-compliance by a source or recipient agency.

d. **Delegated authority.** The Defense Privacy Office shall be responsible for providing professional assistance and administrative support to the Defense Data Integrity Board in carrying out those specific responsibilities of the Board set forth in paragraphs 10b(6) through (10) below.

10. DEFENSE DATA INTEGRITY BOARD

a. **Establishment.** The PA requires the establishment of a Data Integrity Board for each Federal agency that acts as either a source or recipient in a matching program to oversee the agency's participation. Non-Federal governmental entities are not required to have such boards. The Defense Data Integrity Board is established and staffed under reference (b). It is located within the Office of the Director, Administration and Management (ODA&M), (OSD). DON activities participating in computer matching under the Act are encouraged to establish their own subordinate boards if such boards will assist their activity's matching programs. Subordinate boards could secure agreements and cost-benefit analyses from other agencies and perform a preliminary review and evaluation of the DON activity's matching program proposals for the consideration of the Defense Data Integrity Board. Subordinate boards may recommend approval or disapproval of proposed matches, but only the Defense Data Integrity Board, via CNO (OP-09B30), shall have the final approval or disapproval authority of matching agreements within the DOD.

17 JUL 1992

b. Responsibilities of the Defense Data Integrity Board. The Defense Data Integrity Board shall meet at the call of its Executive Secretary and shall meet often enough to ensure that the DOD matching programs are carried out efficiently, expeditiously and in conformance with the PA. The Board may delegate other responsibilities such as compilation of reports, advising program officials and maintaining and disseminating information about the accuracy and reliability of data used in matching. It shall be the responsibility of The Defense Data Integrity board to:

(1) Review matching agreements, approve or disapprove programs based upon the assessment of the adequacy of the agreements and supporting documentation, including cost-benefit analyses, and maintain all written agreements for receipt or disclosure of DOD records to ensure compliance with all relevant statutes, guidelines and regulations.

(2) Review all matching programs in which DOD Components have participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, and agency agreements, and assess the cost and benefits of such programs.

(3) Review all recurring matching programs in which the agency has participated during the past year, either as a source agency or recipient agency, for continued justification for such disclosures.

(4) Review all requests for pilot matches. Approve or disapprove such requests based upon the assessment of the supporting justification.

(5) Review all requests for combining verification and notice requirements.

(6) Compile an annual report, which will be submitted to the Secretary of Defense and the Office of Management and Budget and made available to the public upon request, describing the matching activities of the agency, including:

(a) Matching programs in which the DON activity has participated as either a source agency or a recipient agency.

(b) Matching agreements proposed under subsection (c) of the Act that were disapproved by the Board.

(c) Any changes in the membership or structure of

the Board in the preceding year.

(d) The reasons for any waiver of the requirement for a cost-benefit analysis prior to the approval of a matching program.

(e) Any violations of matching agreements that have been alleged or identified and any corrective action taken.

(f) Any other information required by the Director of the Office of Management and Budget to be included in the report.

(7) Serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs.

(8) Provide interpretation and guidance to DOD Components and personnel on the requirements for matching programs.

(9) Review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section.

(10) Review and report any DOD matching activities that are not matching programs.

11. APPEALS OF DENIALS OF MATCHING AGREEMENTS

a. Disapproval by the Board. If the Defense Data Integrity Board disapproves a matching agreement, a party to the agreement may appeal the disapproval to the Director of the Office of Management and Budget, Washington, D.C. 20503. Appeals must be made within 30 days after the Defense Data Integrity Board's written disapproval. The appealing party shall submit with its appeal the following:

(1) Copies of all documentation accompanying the initial matching agreement proposal.

(2) A copy of the Defense Data Integrity Board's disapproval and reasons therefore.

(3) Evidence supporting the cost-benefit effectiveness of the match.

(4) Any other relevant information, e.g., timing

17 JUL 1992

considerations, public interest served by the match, etc.

b. OMB approval. If the Director of the Office of Management and Budget approves a matching program it will not become effective until 30 days after the Director reports his decision to Congress.

c. Recourse by the Inspector General. If the Defense Data Integrity Board and the Director of the Office of Management and Budget both disapprove a matching program proposed by the Inspector General of the agency, the Inspector General may report that disapproval to the head of the agency and to the Congress.

12. PROPOSALS FOR MATCHING PROGRAMS

a. Who initiates the action. The recipient DON activity (or the DON source agency in a match conducted by a non-Federal agency); or the recipient activity within the DON activity for internal matches, is responsible for reporting the match for approval. The responsible official should contact the other participants to gather the information necessary to make a unified report.

b. New or altered matching programs. Determine if the match is a new program or an existing one. A new match is one for which no public notice has been published in the Federal Register as required by paragraph 4b of this enclosure. An altered matching program is an established (published public notice) match with such a significant change that it requires amendment as described in paragraph 7d of this enclosure. An altered matching program should not be confused with a request for an unchanged extension of an established program as set forth in paragraph 7c of this enclosure.

c. Contents of report (original and one copy)

(1) A proposed new matching program report shall consist of a DON letter of transmittal with the following attached documents:

(a) Completed agreement between the participants (paragraph 7).

(b) Benefit/cost analysis (paragraph 8).

(c) Proposed Federal Register matching notice for public review and comment (paragraph 4d).

17 JUL 1992

(d) Copies of all the appropriate forms (e.g., applications) of the participating parties providing direct notice to the individual (paragraph 4c(1)) or any other means of communication used.

(e) Copy or copies of the appropriate Federal Register system(s) of record notice(s) containing an appropriate routine use providing constructive notice to the individual (paragraph 5c(2)).

(2) A report on a proposed alteration to an established matching program shall consist of a Component letter of transmittal with the following attached documents:

(a) A report containing the significant change(s) (paragraph 7d) and the following additional information:

(1) What alternatives to matching the agencies considered and why a matching program was chosen.

(2) The date the match was approved by each participating Federal agency's Data Integrity Board.

(3) Whether a cost-benefit analysis was required and, if so, whether it projected a favorable ratio.

(b) Proposed Federal Register matching notice for public review and comment (paragraph 5d).

(3) A report requesting an extension beyond 18 months of an established unchanged matching program must be received by the Defense Privacy Office at least 4 months prior to the actual expiration date and consist of a DON letter of transmittal with the following attached:

(a) Justification for the extension (not to exceed one year).

(b) Certification by the participants that the program has been conducted in compliance with the matching agreement.

d. Who receives the reports. Submit all reports to the senior Component PA official. Proposals shall further be reviewed, if applicable, by the Component Data Integrity Board for approval or disapproval recommendations and forwarded to the Defense Privacy Office for consideration by the Defense Data Integrity Board.

17 JUL 1992

e. Action by the Defense Privacy Office. The Defense Privacy Office shall present proposals before the Defense Data Integrity Board which shall either approve or disapprove proposals on their merits. Any inaction based on insufficient data, justification, or supporting documentation shall be returned to the DON activity for any further corrective action deemed necessary. Any disapproved proposals are returned with the stated reasons. See also paragraph 11 of this enclosure. Board approved proposals are coordinated with the Office of the Assistant Secretary of Defense (Legislative Affairs) and the Office of the General Counsel, DOD. The Defense Privacy Office prepares for the signature of the Chairman of the Board (DA&M, OSD), the transmittal letters sent to Congress and OMB and concurrently submits the proposed Federal Register matching notice for publication.

f. Time restrictions on the initiation of new or altered matching programs

(1) All time periods begin from the date the Chairman of the Board signs the transmittal letters.

(2) 60 days must elapse before the matching program may become operational.

(3) The 60 day period for OMB and Congressional review and the 30 day notice and comment period for the Matching Notice shall run concurrently.

g. Requests for waivers. A DON activity may seek waivers of certain matching program requirements including the 60 day-review period by OMB and Congress. Requests for waivers shall be included in the letter of transmittal to the report. Such requests shall cite the specific provision for which a waiver is being requested with full justification showing the reasons and the adverse consequences if a waiver is not granted.

h. Outside review and DON activity. A DON activity may presume OMB and Congressional concurrence if the 60 day review period has run without comment from any reviewer outside the DOD. Under no circumstances shall the matching program be implemented before 30 days have elapsed after publication of the matching notice in the Federal Register. This period cannot be waived.

17 JUL 1992

THE PRIVACY ACT OF 1974
(As Amended)

5 U.S.C. § 552a

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, that this Act may be cited as the "Privacy Act of 1974."

SECTION 2

(a) The Congress finds that --

- (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;
- (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
- (3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
- (4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
- (5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to --

- (1) permit an individual to determine what records

Enclosure (19)

17 JUL 1992

- pertaining to him are collected, maintained, used, or disseminated by such agencies;
- (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
 - (3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
 - (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
 - (5) permit exemptions from such requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
 - (6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

SECTION 3

Title 5, United States Code, is amended by adding after section 552 the following new section:

552a. Records maintained on individuals

(a) DEFINITIONS

For purposes of this section --

- (1) the term "agency" means agency as defined in section 552(e) of this title;
- (2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

Enclosure (19)

17 JUL 1992

- (3) the term "maintain" includes maintain, collect, use, or disseminate;
- (4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;
- (5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;
- (6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;
- (7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;
- (8) the term "matching program" --
 - (A) means any computerized comparison of --
 - (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of --
 - (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with

Enclosure (19)

17 JUL 1992

- (II) respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs, or
 - (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,
- (B) but does not include --
- (i) matches performed to produce aggregate statistical data without any personal identifiers;
 - (ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;
 - (iii) matches performed by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;
 - (iv) matches of tax information --
 - (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986;
 - (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code;
 - (III) for the purpose of intercepting a

Enclosure (19)

17 JUL 1992

- tax refund due an individual under authority granted by section 464 or 1137 of the Social Security Act; or
- (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;
- (v) matches --
- (I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or
- (II) conducted by an agency using only records from systems of records maintained by that agency;
- if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or
- (vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;
- (9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

Enclosure (19)

17 JUL 1992

- (10) the term "non-Federal agency" means 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 matching program;
- (11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;
- (12) the term "Federal benefit program" means any 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; and
- (13) the term "federal personnel" means 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 Government of the United States (including survivor benefits).

(b) CONDITIONS OF DISCLOSURE

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
- (2) required under section 552 of this title;
- (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
- (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity

Enclosure (19)

17 JUL 1992

pursuant to the provisions of title 13;

- (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
- (6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or his designee to determine whether the record has such value;
- (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
- (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
- (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
- (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
- (11) pursuant to the order of a court of competent jurisdiction; or
- (12) to a consumer reporting agency in accordance with section 3711(f) of title 31.

Enclosure (19)

17 JUL 1992

(c) ACCOUNTING OF CERTAIN DISCLOSURES

Each agency, with respect to each system of records under its control, shall --

- (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of --
 - (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section;
 - (B) the name and address of the person or agency to whom the disclosure is made;
- (2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;
- (3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and
- (4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) ACCESS TO RECORDS

Each agency that maintains a system of records shall --

- (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

17 JUL 1992

- (2) permit the individual to request amendment of a record pertaining to him and --
 - (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and
 - (B) promptly, either --
 - (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or
 - (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;
- (3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;
- (4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide

Enclosure (19)

17 JUL 1992

copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

- (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) AGENCY REQUIREMENTS

Each agency that maintains a system of records shall --

- (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;
- (2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;
- (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual --
 - (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether the disclosure of such information is mandatory or voluntary;
 - (B) the principal purpose or purposes for which the information is intended to be used;
 - (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and
 - (D) the effects on him, if any, of not providing all or any part of the requested information;
- (4) subject to the provisions of paragraph (11) of this

Enclosure (19)

SECNAVINST 5211.5D
17 JUL 1992

subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include --

- (A) the name and location of the system;
 - (B) the categories of individuals on whom records are maintained in the system;
 - (C) the categories of records maintained in the system;
 - (D) each routine use of the records maintained in the system, including the categories of users and the purpose of such use;
 - (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
 - (F) the title and business address of the agency official who is responsible for the system of records;
 - (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
 - (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
 - (I) the categories of sources of records in the system;
- (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;
- (6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of

Enclosure (19)

this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

- (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;
- (8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;
- (9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;
- (10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;
- (11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and
- (12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) AGENCY RULES

Enclosure (19)

17 JUL 1992

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall--

- (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;
- (2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;
- (3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;
- (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and
- (5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g) CIVIL REMEDIES

- (1) Whenever any agency --
 - (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record

Enclosure (19)

17 JUL 1992

in accordance with his request, or fails to make such review in conformity with that subsection;

- (B) refuses to comply with an individual request under (d)(1) of this section;
- (C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or
- (D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

- (2) (A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such case the court shall determine the matter de novo.
- (B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.
- (3) (A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in

17 JUL 1992

camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

- (B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.
- (4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of --
- (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and
 - (B) the costs of the action together with reasonable attorney fees as determined by the court.
- (5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where any agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to the effective date of this section.

Enclosure (19)

17 JUL 1992

(h) RIGHTS OF LEGAL GUARDIANS

For the purpose of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i) CRIMINAL PENALTIES

- (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

(j) GENERAL EXEMPTIONS

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1), and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is --

- (1) maintained by the Central Intelligence Agency; or
- (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws,

17 JUL 1992

including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional probation, pardon, or parole authorities, and which consists of --

- (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, parole and probation status;
- (B) information compiled for the purpose of a criminal investigation; including reports of informants and investigations, and associated with an identifiable individual; or
- (C) reports identifiable to an individual compiled at any stage of the process of enforcement of criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) SPECIFIC EXEMPTIONS

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is --

- (1) subject to the provisions of section 552(b)(1) of this title;
- (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such

Enclosure (19)

17 JUL 1992

material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

- (3) maintained in connection with providing protection services to the President of the United States or other individuals pursuant to section 3056 of title 18;
- (4) required by statute to be maintained and used solely as statistical records;
- (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or
- (7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section

Enclosure (19)

17 JUL 1992

553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(1) ARCHIVAL RECORDS

- (1) Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.
- (2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.
- (3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m) GOVERNMENT CONTRACTORS

- (1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall,

Enclosure (19)

17 JUL 1992

consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

- (2) A consumer reporting agency to which a record is disclosed under section 3711(f) of title 31 shall not be considered a contractor for purposes of this section.

(n) MAILING LISTS

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) MATCHING AGREEMENTS

- (1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying --
- (A) the purpose and legal authority for conducting the program;
 - (B) the justification for the program and the anticipated results, including a specific estimate of any savings;
 - (C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;
 - (D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance

Enclosure (19)

17 JUL 1992

provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to --

- (i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and
 - (ii) applicants for and holders of positions as Federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;
- (E) procedures for verifying information produced in such matching program as required by subsection (p);
 - (F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
 - (G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
 - (H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
 - (I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
 - (J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
 - (K) that the Comptroller General may have access to all records of a recipient agency or non-Federal

Enclosure (19)

17 JUL 1992

agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

- (2) (A) A copy of each agreement entered into pursuant to paragraph (1) shall --
 - (i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and
 - (ii) be available upon request to the public.
- (B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).
- (C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.
- (D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if --
 - (i) such program will be conducted without any change; and
 - (ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS

- (1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit

Enclosure (19)

SECNAVINST 5211.5D
17 JUL 1992

program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until--

- (A) (i) the agency has independently verified the information; or
 - (ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that --
 - (I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and
 - (II) there is a high degree of confidence that the information provided to the recipient agency is accurate;
 - (B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and
 - (C) (i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or
 - (ii) in the case of a program for which no time period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.
- (2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual,

Enclosure (19)

17 JUL 1992

including, where applicable, investigation and confirmation of --

- (A) the amount of any asset or income involved;
 - (B) whether such individual actually has or had access to such asset or income for such individual's own use; and
 - (C) the period or periods when the individual actually had such asset or income.
- (3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) SANCTIONS

- (1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency of non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.
- (2) No source agency may renew a matching agreement unless--
- (A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and
 - (B) the source agency has no reason to believe that the certification is inaccurate.

(r) REPORT ON NEW SYSTEMS AND MATCHING PROGRAMS

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental

17 JUL 1992

Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable effect of such proposal on the privacy or other rights of individuals.

(s) BIENNIAL REPORT

The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report --

- (1) describing the actions of the Director of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;
- (2) describing the exercise of individual rights of access and amendment under this section during such years;
- (3) identifying changes in or additions to systems of records;
- (4) containing other such information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t) EFFECT OF OTHER LAWS

Relationship of the Privacy Act to the Freedom of Information Act.

- (1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.
- (2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) DATA INTEGRITY BOARDS

- (1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of

Enclosure (19)

17 JUL 1992

such agency the agency's implementation of this section.

- (2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.
- (3) Each Data Integrity Board --
 - (A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;
 - (B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, and agency agreements, and assess the cost and benefits of such programs;
 - (C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;
 - (D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including--
 - (i) matching programs in which the agency has participated as a source agency or recipient agency;
 - (ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

17 JUL 1992

- (iii) any changes in the membership or structure of the Board in the preceding year;
 - (iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
 - (v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and
 - (vi) any other information required by the Director of the Office of Management and Budget to be included in such report;
- (E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;
- (F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;
- (G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and
- (H) may review and report on any agency matching activities that are not matching programs.
- (4) (A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.
- (B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the

Enclosure (19)

17 JUL 1992

Office of Management and Budget, that a cost-benefit analysis is not required.

- (C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.
- (5) (A) If a matching agreement is disapproved by a Data Integrity Board, any party to such an agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.
- (B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that--
 - (i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;
 - (ii) there is adequate evidence that the matching agreement will be cost-effective; and
 - (iii) the matching program is in the public interest.
- (C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).
- (D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector

Enclosure (19)

17 JUL 1992

general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

- (6) The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3)(D). Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and submission of a cost-benefit analysis and the reasons for granting the waiver.
- (7) In the reports required by paragraphs (3)(D) and (6), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) OFFICE OF MANAGEMENT AND BUDGET RESPONSIBILITIES

The Director of the Office of Management and Budget shall--

- (1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and
- (2) provide continuing assistance to and oversight of the implementation of this section by agencies.

SECTION 6 [Repealed]

SECTION 7

- (a) (1) It shall be unlawful for any Federal, state, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.
- (2) the provisions of paragraph (1) of this subsection

Enclosure (19)