

APPENDIX A

April 8, 1992

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
INSPECTOR GENERAL
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1

This memorandum reissues the Defense Privacy Board Advisory Opinions. Former Opinions 14, 15, 28 and 40 have been withdrawn. Those opinions addressed Freedom of Information Act issues as opposed to Privacy Act matters. The enclosed opinions have been renumbered and should be substituted for those previously issued by the Defense Privacy Board.

[signed]

D.O. Cooke
Director

Enclosure

THIS PAGE LEFT BLANK INTENTIONALLY

DEFENSE PRIVACY BOARD

ADVISORY OPINIONS

DEFENSE PRIVACY OFFICE
1941 JEFFERSON DAVIS HIGHWAY
CRYSTAL MALL 4, ROOM 920
ARLINGTON, VA 22202-4502
(703) 607-2943
DSN 327-3943

THIS PAGE LEFT BLANK INTENTIONALLY

TABLE OF CONTENTS

	Page
1. PROVIDING WAGE AND EARNING STATEMENTS (W-2 FORMS) OF MILITARY PERSONNEL TO STATE AND LOCAL TAXING AUTHORITIES	A-9
2. PRIVACY RIGHTS AND DECEASED PERSONS	A-9
3. DISCLOSURE OF RECORDS FROM A SYSTEM OF RECORDS TO THE NEXT OF KIN OF PERSONS MISSING IN ACTION OR OTHERWISE UNACCOUNTED FOR	A-10
4. CORRECTIONS OF MILITARY RECORDS UNDER THE PRIVACY ACT	A-11
5. APPLICABILITY OF THE PRIVACY ACT TO NATIONAL GUARD RECORDS	A-11
6. ASSESSING FEES TO MEMBERS OF CONGRESS FOR FURNISHING RECORDS WHICH ARE SUBJECT TO THE PRIVACY ACT	A-12
7. DISCLOSURE OF HOME OF RECORD TO MEMBERS OF CONGRESS	A-12
8. ACCOUNTING FOR DISCLOSURES OF RECORDS THROUGH MILITARY LEGISLATIVE LIAISON CHANNELS	A-13
9. THE PRIVACY ACT AND MINORS	A-13
10. DISCLOSURE OF IDENTITIES OF CONFIDENTIAL SOURCES FROM INVESTIGATIVE RECORDS EXEMPTED UNDER SUBSECTION (k)(2)	A-14
11. APPLICATION OF THE PRIVACY ACT TO INFORMATION IN HOSPITAL COMMITTEE MINUTES	A-14
12. ACCOUNTING FOR MASS DISCLOSURES OF RECORDS TO OTHER AGENCIES	A-14
13. DISCLOSURE OF RECORDS TO STATE AGENCIES TO VALIDATE UNEMPLOYMENT COMPENSATION CLAIMS OF FORMER FEDERAL EMPLOYEES AND MILITARY MEMBERS	A-15
14. DISCLOSURE OF RECORDS TO FINANCIAL INSTITUTIONS	A-15
15. DISCLOSURE OF PHOTOGRAPHS IN THE CUSTODY OF THE DEPARTMENT OF	A-16

DEFENSE

	Page
16. DISCLOSURE OF RECORDS FROM SYSTEMS OF RECORDS TO A CONTRACTOR PURSUANT TO A CONTRACT	A-16
17. DEFINITION OF AN "AGENCY OR INSTRUMENTALITY OF ANY JURISDICTION WITHIN OR UNDER THE CONTROL OF THE UNITED STATES"	A-17
18. LOCATION OF PRIVACY ACT ADVISORY STATEMENTS	A-17
19. PRIVACY ACT ADVISORY STATEMENTS FOR INSPECTOR GENERAL COMPLAINT FORMS	A-17
20. RECRUITMENT ADVERTISEMENTS IN THE PUBLIC MEDIA	A-18
21. INFORMATION REQUESTED IN THE PUBLIC DOMAIN	A-18
22. IMPLICATIONS ON VARIOUS METHODS OF DISTRIBUTING LEAVE AND EARNING STATEMENTS	A-19
23. THE APPEARANCE OF THE SOCIAL SECURITY NUMBER IN THE WINDOW OF AN ENVELOPE CONTAINING RECORD INFORMATION DOES NOT CONSTITUTE A DISCLOSURE	A-19
24. WHAT CONSTITUTES A PRIVACY ACT REQUEST FOR ACCESS OR AMENDMENT FOR PURPOSES OF COMPLIANCE WITH PROCESSING AND REPORTING REQUIREMENTS	A-19
25. INFORMATION PERTAINING TO THIRD PARTIES MAY NOT BE PROTECTED BY THE PRIVACY ACT	A-20
26. DISCLOSURE OF SECURITY CLEARANCE LEVEL	A-20
27. PRIVACY ACT APPLICABILITY TO LEGAL MEMORANDA MAINTAINED IN A SYSTEM OF RECORDS	A-20
28. THE PRIVACY ACT DOES NOT APPLY TO FILES INDEXED BY NON-PERSONAL IDENTIFIERS AND RETRIEVED BY MEMORY	A-21
29. DEPERSONALIZING COMPUTER CARDS AND PRINTOUTS BEFORE DISPOSAL	A-21
30. NO SUPPLEMENTAL CHARGES MAY BE ASSESSED FOR UNLISTED TELEPHONE	A-21

NUMBER SERVICE ON INSTALLATIONS WHERE NO COMMERCIAL SERVICE IS AVAILABLE

	Page
31. THE PRIVACY ACT GENERAL EXEMPTION DOES NOT FOLLOW THE RECORD	A-21
32. THE PRIVACY ACT SYSTEM NOTICE REQUIREMENT APPLIES TO COURT-MARTIAL FILES	A-22
33. A ROUTINE USE IS NOT REQUIRED FOR DISCLOSURE OF DEPARTMENT OF DEFENSE RECORDS TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION AND TO THE GENERAL SERVICES ADMINISTRATION	A-22
34. DEFINITION OF "ORDER OF A COURT OF COMPETENT JURISDICTION"	A-23
35. RECORDS MAY BE DISCLOSED TO SERVICE-ORIENTED SOCIAL WELFARE ORGANIZATIONS PURSUANT TO AN ESTABLISHED ROUTINE USE	A-23
36. PRIVACY ACT WARNING LABELS	A-24
37. DISCLOSURE OF RECORDS CONCERNING CHARITABLE CONTRIBUTIONS OR PARTICIPATION IN SAVINGS BOND PROGRAMS	A-24
38. PERSONAL NOTES AS RECORDS WITHIN A SYSTEM OF RECORDS	A-24
39. REQUIREMENT FOR PRIVACY ACT ADVISORY STATEMENTS FOR ADMINISTRATIVE PROCEEDINGS	A-25
40. ACCESS TO MEDICAL RECORDS BY INDIVIDUALS WHO COULD BE ADVERSELY AFFECTED	A-25
41. NO REQUIREMENT TO PROVIDE PRIVACY ACT ADVISORY STATEMENTS TO LABOR ORGANIZATIONS	A-26
42. INFORMATION ON FORMS ATTACHED TO SECURITY CONTAINERS OR FACILITIES IS SUBJECT TO THE PRIVACY ACT	A-26
43. VERIFYING THE ACCURACY OF PERSONAL DATA IN A RECORD IS SUBJECT TO THE PRIVACY ACT	A-27
44. ONE DEPARTMENT OF DEFENSE COMPONENT MAY DISCLOSE HEALTH CARE RECORDS TO ANOTHER WITHOUT A ROUTINE USE OR CONSENT	A-27

45. DISCLOSURE OF THE ORIGINAL, PRE-1968, SERIAL NUMBER (SERVICE NUMBER) ASSIGNED TO MILITARY PERSONNEL

A-28

	Page
46. THE SOCIAL SECURITY NUMBER ON BUILDING AND INSTALLATION BADGES	A-28
47. USING BOTH GENERAL AND SPECIFIC PRIVACY ACT EXEMPTIONS FOR THE SAME SYSTEM OF RECORDS	A-28
48. DISCLOSURE OF INFORMATION IN BLANKET ORDERS	A-29

1. **PROVIDING WAGE AND EARNING STATEMENTS (W-2 FORMS) OF MILITARY PERSONNEL TO STATE AND LOCAL TAXING AUTHORITIES**

A blanket routine use has been established for all Department of Defense (DoD) systems of records which permits disclosure of information contained in W-2 forms to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C. §§ 5516, 5517 and 5520. Accounting for disclosures made pursuant to this routine use is required by the Privacy Act. See 5 U.S.C. § 552a(c). Defense Privacy Board Advisory Opinion 12 contains guidance on accounting for mass disclosures.

2. **PRIVACY RIGHTS AND DECEASED PERSONS**

The Privacy Act and its legislative history are silent as to whether a decedent is an individual and whether anyone else may exercise the decedent's rights concerning records pertaining to him or her maintained by agencies. The Privacy Act's failure to provide specifically for the exercise of rights on behalf of decedents, coupled with the personal judgment implicitly necessary to exercise such rights, indicates that the Act did not contemplate permitting relatives and other interested parties to exercise Privacy Act rights after the death of the record subject. See Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28951 (July 9, 1975).

Whether access to records pertaining to a decedent should be permitted under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, depends on the circumstances in each particular case. The FOIA would permit an agency to withhold if:

- a. In the case of "personnel and medical and similar files, the disclosure . . . would be a clearly unwarranted invasion of personal privacy" under 5 U.S.C. § 552(b)(6); or
- b. In the case of law enforcement investigatory records, the disclosure would "constitute an unwarranted invasion of personal privacy" under 5 U.S.C. § 552(b)(7)(C).

Demise of a record subject (ending Privacy Act protection which permits disclosure only when required by the FOIA) does not mean the privacy-protective features of the FOIA no longer apply. Public interest in disclosure must be balanced against the degree of invasion of personal privacy. An agency need not automatically, in all cases, "disclose inherently private information as soon as the individual dies, especially when the public's interest in the information is minimal." Kiraly v. Federal Bureau of Investigation, 728 F.2d 273, 277 (6th Cir. 1984).

As a final point, a decedent's records may pertain as well to other living individuals, and to the extent that the records are retrieved by their personal identifiers, their Privacy Act rights remain in effect. As to any records of a decedent requested under the FOIA, the degree to which the personal privacy of the decedent's relatives, or anyone else to whom the records pertain would be invaded must be considered in the FOIA balancing test mentioned above. See DoD 5400.7-R, paragraph 3-200, no. 6.

In applying the FOIA balancing test to the records of those individuals who remain missing or unaccounted for as a result of the Vietnam conflict, the privacy sensibilities of their family members should be considered as a clear and present factor that weighs against the public release of information.

The release of information regarding these records should be limited to basic information such as name, rank, date of loss, country of loss, current status, home of record (city and state), and any other privacy information that the primary next of kin has consented to releasing.

3. **DISCLOSURE OF RECORDS FROM A SYSTEM OF RECORDS TO THE NEXT OF KIN OF PERSONS MISSING IN ACTION OR OTHERWISE UNACCOUNTED FOR**

A legal guardian appointed by a court of competent jurisdiction for a member missing in action or otherwise unaccounted for would be in the position of the member and have the same rights as the member. 5 U.S.C. § 552a(h). In such a case, records contained in a system of records and relating to the missing member may be disclosed to third persons upon the written consent of the guardian. If no guardian has been appointed or an appointed guardian does not give written consent, such records may be disclosed only if authorized by 5 U.S.C. § 552a(b).

For example, information relating to persons missing in action or otherwise unaccounted for may be disclosed "pursuant to the order of a court of competent jurisdiction." 5 U.S.C. § 552a(b)(11). [For a discussion of "order of a court of competent jurisdiction," see Defense Privacy Board Advisory Opinion 37.] In a case involving the families of military personnel missing in action, one court ordered, in part, that next of kin receiving governmental financial benefits which could be terminated by a status review be afforded "reasonable access to the information upon which the status review will be based." McDonald v. McLucas, 371 F. Supp. 831, 836 (S.D.N.Y. 1974). Since a status review is likely to require access to almost all significant information in a system of records pertaining to a member missing in action, this order constitutes sufficient authority under the Privacy Act for disclosure of almost any personal records of interest.

Information in a system of records also may be available to any person under the Freedom of Information Act (FOIA) if disclosure of the records concerned does not constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6); 5 U.S.C. § 552a(b)(2). In determining what information must be disclosed under this standard, a balancing test weighing the public interest in disclosure against the potential invasion of personal privacy should be conducted. See DoD 5400.7-R, paragraph 3-200, No. 6. See, e.g., Department of the Air Force v. Rose, 425 U.S. 352, 96 S. Ct. 1592, 48 L. Ed.2d 11 (1976); Church of Scientology v. Department of Defense, 611 F.2d 738 (9th Cir. 1979). Because facts and needs will differ in each case, the balancing test may require disclosure of information in one circumstance but not in another. See Getman v. National Labor Relations Board, 450 F.2d 670 (D.C. Cir. 1971); Robles v. Environmental Protection Agency, 484 F.2d 843 (4th Cir. 1973); Wine Hobby, USA, Inc. v. Bureau of Alcohol, Tobacco and Firearms, 502 F.2d 133 (3rd Cir. 1974).

Due to the unusual circumstances involved when a service member is missing in action or otherwise

unaccounted for, next of kin may have a more compelling case for disclosure of a requested record than would other third parties. However, each request must be evaluated on its own merits.

Should the record subject's status be changed to "deceased," see Defense Privacy Board Advisory Opinion 2 concerning application of the Privacy Act and FOIA to decedents' records.

4. CORRECTIONS OF MILITARY RECORDS UNDER THE PRIVACY ACT

One main purpose of the Privacy Act is to ensure records pertaining to individuals are maintained accurately so informed decisions based on those records can be made. The Privacy Act amendment provision, 5 U.S.C. § 552a(d)(2), permits individuals to request factual amendments to records pertaining to them. It does not permit correction of judgmental decisions such as efficiency reports or selection and promotion board reports. These judgmental decisions may be challenged before the Boards for Correction of Military and Naval Records which by statute are authorized to make these determinations. 10 U.S.C. § 1552. If factual matter is corrected under Privacy Act procedures, subsequent judgmental decisions that may have been affected by the factual correction, if contested, should be considered by the Boards for Correction of Military and Naval Records.

5. APPLICABILITY OF THE PRIVACY ACT TO NATIONAL GUARD RECORDS

As defined in the Privacy Act, "maintain" includes various record-keeping functions to which the Act applies; i.e., maintaining, collecting, using, and disseminating. In turn, this connotes control over and responsibility and accountability for systems of records. 5 U.S.C. § 552a(a)(3); Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28954 (July 9, 1975) (OMB Guidelines).

Reserve components of the Army and the Air Force include the Army and Air National Guards of the United States respectively, which are composed of federally recognized units and organizations of the Army or Air National Guard and members of the Army or Air National Guard who are also Reserves of the Army or Air Force. 10 U.S.C. §§ 3077 and 8077. 10 U.S.C. § 275 requires the Departments of the Army and the Air Force to maintain personnel records on all members of the federally recognized units and organizations of the Army and Air National Guards and on all members of the Army or Air National Guards who are also reserves of the Army and Air Force. Such records are "maintained" by the Army or Air Force for the purposes of the Privacy Act. These records are not all located at the National Guard Bureau. Some are in the physical possession of the state adjutant general. However, records need not be physically located in the agency for them to be maintained by the agency. See OMB Guidelines. Records located at the state level are under the direct control of the Army and Air Force in that they are maintained by the state under regulations (NGR 600-200 and AFR 35-44) implementing 10 U.S.C. § 275, and promulgated by authority of the Secretaries of the Army and the Air Force under 10 U.S.C. § 280. Therefore, the records are Army or Air Force records and subject to the provisions of the Privacy Act.

That the records are subject to the Privacy Act does not mean they cannot be used by the members of the state national guards. The state officials using and maintaining the records are members of the reserves (members of the Army or Air Force National Guard of the United States). Disclosure to them in performance of their duties is disclosure within the Department of Defense not requiring a published routine use or an accounting.

6. ASSESSING FEES TO MEMBERS OF CONGRESS FOR FURNISHING RECORDS WHICH ARE SUBJECT TO THE PRIVACY ACT

The Privacy Act authorizes an agency to "establish fees to be charged, if any, to any individual for making copies of his record . . ." 5 U.S.C. § 552a(f)(5). Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28968 (July 9, 1975) and DoD 5400.11-R each point out that a fee may be charged for only the direct cost of making the copy. This guidance also states that if copying is the only means whereby the record can be made available to the individual, reproduction fees will not be assessed.

Therefore, charging fees is discretionary. However, as a general policy, the Department of Defense should not charge Members of Congress for records furnished when requested under the Privacy Act, unless the charge would be substantial. In no event should a fee less than \$30.00 be determined substantial. In the case of constituent inquiries involving a substantial fee, a suggestion may be made that the Member of Congress advise the constituent that the information may be obtained by writing the appropriate office and paying reproduction costs. Additionally, the record may be examined at no cost if the constituent wishes to visit the record custodian.

7. DISCLOSURE OF HOME OF RECORD TO MEMBERS OF CONGRESS

The blanket routine use provisions for Department of Defense (DoD) systems of records, first published on October 9, 1975, at 40 Fed. Reg. 47748, are sufficiently broad to permit the disclosure of home of record information to a Member of Congress or Congressional staff member who is making an inquiry of a DoD component at the request of the subject service member, even if the subject member's request did not concern that particular portion of the service record.

However, the service record entry for home of record is intended to reflect the member's home at the time of entry into service or order to active duty. The Member of Congress or Congressional staff member may be more interested in the service member's legal residence for voting purposes or as entered on a W-4 form and as reflected by the member's pay record. Disclosure of home of record information to a Member of Congress or a Congressional staff member should include a caveat that it reflects only the home address at the time of entry into service or order to active duty.

8. ACCOUNTING FOR DISCLOSURES OF RECORDS THROUGH MILITARY LEGISLATIVE LIAISON CHANNELS

Procedures and divisions of responsibility should be established by military departments to ensure preparation of required accountings when information concerning individuals is disclosed to Members of Congress. Whether disclosure is made pursuant to an established routine use or prior written consent of the record subject, an accounting must be kept. See 5 U.S.C. § 552a(c). When a disclosure is made directly to a Member of Congress by the custodian of the record, that activity is responsible for keeping an appropriate accounting. However, a more difficult administrative problem arises when requested information is transmitted by the custodian to the legislative liaison activity for re-transmittal and the latter either deletes from or adds to information originally provided. In such cases it might be impossible for the custodian to keep an accurate accounting of what actually was disclosed to the Congressional office unless the legislative liaison office provides feedback.

The problem should not be resolved on a DoD-wide scale because the formulation of specific procedures for disclosure accounting will involve consideration of a number of factors which will vary among the military departments and other DoD components. The factors include internal organizational relationships, the components' prescribed methods and responsibilities for responding to Congressional inquiries, and possibly the characteristics of the particular records and record systems involved.

The liaison activity should prepare a disclosure accounting and forward it to the custodian. The accounting should contain the name and address of the person to whom the disclosure was made and the Member of Congress for whom he or she works, as well as the date, nature and purpose of the disclosure. The name, rank, title and duty address of the person making the disclosure also should be included. The accounting must be kept for five years or the life of the record, whichever is longer.

9. THE PRIVACY ACT AND MINORS

The Privacy Act applies to any "individual" which is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2). With respect to any rights granted the individual, no restriction is imposed on the basis of age; therefore, minors have the same rights and protections under the Privacy Act as do adults.

The Privacy Act provides that "the parent of any minor . . . may act on behalf of the individual." 5 U.S.C. § 552a(h). This subsection ensures that minors have a means of exercising their rights under the Privacy Act. Office of Management and Budget Privacy Act Guidelines (OMB Guidelines), 40 Fed. Reg. 28949, 28970 (July 9, 1975). It does not preclude minors from exercising rights on their own behalf, independent of any parental exercise. Parental exercise of the minor's Privacy Act rights is discretionary. A Department of Defense (DoD) component may permit parental exercise of a minor's Privacy Act rights at its discretion, but the parent has no absolute right to exercise the minor's rights absent a court order or the minor's consent. See OMB Guidelines, 40 Fed. Reg. 56741, 56742 (December 4, 1975). Further, the parent exercising a minor's rights under the Privacy Act must be doing so on behalf of the minor and not merely for the parent's benefit. DePlanche v. Califano, 549 F.

Supp. 685 (W.D. Mich. 1982).

The age at which an individual is no longer a minor becomes crucial when an agency must determine whether a parent may exercise the individual's Privacy Act rights. With respect to records maintained by DoD components, the age of majority is 18 years unless a court order states otherwise or the individual, at an earlier age, marries, enlists in the military, or takes some other action that legally signifies attainment of majority status. Once an individual attains the age of majority, Privacy Act rights based solely on parenthood cease.

10. DISCLOSURE OF IDENTITIES OF CONFIDENTIAL SOURCES FROM INVESTIGATIVE RECORDS EXEMPTED UNDER SUBSECTION (k)(2)

If a system of records has been exempted under subsection (k)(2) of the Privacy Act, information that would identify a confidential source may be withheld from an individual requesting access to the record under the Privacy Act. 5 U.S.C. § 552a(k)(2). Only information that would not reveal the identity of a confidential source automatically becomes accessible under the Privacy Act when the record subject is denied a right, benefit or privilege.

The Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28973 (July 9, 1975), contain language from the Congressional Record suggesting that the record subject can learn the "substance and source of confidential information" if that information is used to deny him some right, benefit or privilege. However, such language does not refer to Privacy Act compliance. It refers to the possibility that revealing the identity of the confidential source might be required by due process or discovery rules in the course of an administrative or judicial challenge to an adverse action based on information supplied by the source.

11. APPLICATION OF THE PRIVACY ACT TO INFORMATION IN HOSPITAL COMMITTEE MINUTES

The Privacy Act grants access to records contained in systems of records. 5 U.S.C. § 552a(d)(1). To qualify as a "system of records," the information must be retrieved by an individual's name or other identifying particular. 5 U.S.C. § 552a(a)(5). Hospital committee minutes not filed or indexed under an individual's name or other identifying particular are not within a system of records subject to the Privacy Act. Hence, access to those minutes may be denied the individual requesting them under that statute.

12. ACCOUNTING FOR MASS DISCLOSURES OF RECORDS TO OTHER AGENCIES

It is inappropriate to enter into inter-agency support agreements negating the requirement to keep an accounting of disclosures made from systems of records. Except for disclosures made within the

agency or pursuant to the Freedom of Information Act, each agency must keep an accurate accounting of all disclosures made from systems of records under its control. 5 U.S.C. § 552a(c).

Neither the Privacy Act nor the Office of Management and Budget Privacy Act Guidelines, however, specify a form for maintaining the accounting. See 40 Fed. Reg. 28949, 28956 (July 9, 1975). They require only that an accounting be maintained, that it be available to the individual to whom the record pertains, that it be used to advise previous recipients of corrections to records, and that it be maintained so a disclosure of records may be traced to the records disclosed. Individual records need not be marked to reflect disclosure unless necessary to satisfy this tracing requirement.

With respect to mass disclosures, if disclosures are of all records or all of a category of records, it is sufficient simply to identify the category of records disclosed, including the other information required under 5 U.S.C. § 552a(c), in a comprehensible form and make it available as required. Similarly, if disclosures occur at fixed intervals, a statement to that effect, as opposed to a statement at each occasion of disclosure, will satisfy the accounting requirement. If a mass disclosure is not of a complete category of records but, for example, of a random selection within a category, then the above information with a list of individuals whose records were disclosed could be maintained. Appropriate officials then could review this list to provide information to satisfy accounting provisions of the Act.

13. DISCLOSURE OF RECORDS TO STATE AGENCIES TO VALIDATE UNEMPLOYMENT COMPENSATION CLAIMS OF FORMER FEDERAL EMPLOYEES AND MILITARY MEMBERS

Federal agencies, under specific circumstances, are required to disclose records to state agencies administering unemployment compensation claims for former federal civilian employees and military members. Such information includes period of military service, pay grade or amount of federal wages and allowances, reasons for termination of federal service or discharge from military service, and conditions under which a military discharge or resignation occurred. 5 U.S.C. § 8506 and § 8523; 20 C.F.R. § 614.

14. DISCLOSURE OF RECORDS TO FINANCIAL INSTITUTIONS

Information concerning a military member's rank, date of rank, salary, present and past duty assignments, future assignments which have been finalized, office telephone number, office address, length of military service, and duty status may be disclosed to any person requesting such information under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and subsection (b)(2) of the Privacy Act, 5 U.S.C. § 552a, if the information is not classified and disclosure is in conformity with Defense Privacy Board Advisory Opinions 14 and 15.

The Federal Personnel Manual (FPM) authorizes disclosure of information concerning a federal civilian employee's present and past position descriptions, grades, salaries, and duty stations (including office address) to any person under the FOIA if the information is not classified. The FPM further provides

that credit firms may be provided more detailed information concerning tenure of employment, Civil Service status, length of service in the agency and the federal government, and certain information concerning separation of an employee.

When disclosure of particular information requested by a credit bureau would not be authorized under provisions described above, information about individuals may be disclosed from military or civilian personnel records by Department of Defense components with written consent of the subject employee or military member specifically authorizing the disclosure of the requested information. 5 U.S.C. § 552a(b).

15. DISCLOSURE OF PHOTOGRAPHS IN THE CUSTODY OF THE DEPARTMENT OF DEFENSE

Photographs of members of the armed forces and Department of Defense employees taken for official purposes usually may be disclosed when requested under the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a(b)(2), unless the photograph depicts matters that, if disclosed to public view, would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552(b)(6). Generally, award ceremony photographs, selection file photographs, chain of command photographs and similar photographs may be disclosed. Taking such photographs is not collection of information under 5 U.S.C. § 552a(e)(3), so a Privacy Act advisory statement is not required.

16. DISCLOSURE OF RECORDS FROM SYSTEMS OF RECORDS TO A CONTRACTOR PURSUANT TO A CONTRACT

When an agency contracts for operation of a system of records to accomplish an agency function, the contract must cause the Privacy Act to apply to the system of records. Thus, the contractor and the contractor's employees will be considered to be employees of the agency and subject to the provisions of the Privacy Act. 5 U.S.C. § 552a(m).

The Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28976 (July 9, 1975), state that the sole purpose of the contract might not be to operate a system of records, but the contract normally would provide that the contractor operate such a system as a specific requirement of the contract. If the contract can be performed only by operating a system of records, subsection (m) applies even though the contract does not provide expressly for operation of a system of records.

If the contract meets the requirements of subsection (m), the system of records operated by the contractor is deemed to be operated by the agency. Hence, disclosure of records to the contractor is authorized under 5 U.S.C. § 552a(b)(1) when the contract requires the contractor, explicitly or implicitly, to maintain a system of records to perform an agency function.

17. DEFINITION OF AN "AGENCY OR INSTRUMENTALITY OF ANY JURISDICTION WITHIN OR UNDER THE CONTROL OF THE UNITED STATES"

For purposes of nonconsensual disclosures of records from systems of records under 5 U.S.C. § 552a(b)(7), "agency or instrumentality of any jurisdiction within or under the control of the United States" includes any federal agency or unit wherever located and any state or local government agency or unit within the United States legally authorized to enforce civil or criminal laws. The types of agencies or units that may receive records under subsection (b)(7) are as numerous as the entities legally authorized to enforce civil or criminal laws. Such agencies or units may include a city dogcatcher charged with enforcing animal control laws, a county tax collector charged with enforcing county tax laws, a state governor charged with enforcing all state laws, and the Director of the Federal Bureau of Investigation charged with enforcing federal laws.

18. LOCATION OF PRIVACY ACT ADVISORY STATEMENTS

Placement of the Privacy Act advisory statement in a form should be in the following order of preference:

- a. Below the title of the form and positioned so the individual will be advised of the requested information,
- b. Within the body of the form with a notation of its location below the title of the form,
- c. On the reverse of the form with a notation of its location below the title of the form,
- d. Attached to the form as a tear-off sheet, or
- e. Issued as a separate supplement to the form.

19. PRIVACY ACT ADVISORY STATEMENTS FOR INSPECTOR GENERAL COMPLAINT FORMS

Under 5 U.S.C. § 552a(e)(3), a Privacy Act advisory statement is required for Inspector General complaint forms. The agency does not initiate a request for information from an individual, but asks for certain information in order only to respond to a complaint which was initiated voluntarily by an individual. Taking action based on information volunteered by an individual does not eliminate the need for a Privacy Act advisory statement.

Implicit in providing a Privacy Act advisory statement is the notion of informed consent. An individual should be provided sufficient advice about a request for information to make an informed decision about whether or not to respond. See Office of Management and Budget Privacy Act Guidelines, 40 Fed.

Reg. 28949, 28961 (July 9, 1975). The intent of the Privacy Act is to advise individuals requested to provide information about themselves for a system of records about the authority for collecting the information, the uses to be made of it, whether it is voluntary or mandatory to provide it, and the consequences of not providing it. Whenever an agency asks individuals for information about themselves for a system of records, a Privacy Act advisory statement must be provided. There is no difference between an Inspector General complaint which triggers a request for information and a medical form completed only after an individual voluntarily initiates a request for treatment. All agencies have determined that all medical forms require Privacy Act advisory statements.

20. RECRUITMENT ADVERTISEMENTS IN THE PUBLIC MEDIA

Published coupons and business return postcards are used as a means for an individual to request from the military service information concerning a particular recruiting program, and they usually contain blanks for the individual's name, address, telephone number, date and place of birth, level of education, degrees received, and the most recent previous educational agency or institution attended. If the coupon or postcard is used solely to fulfill the individual's request for information and then promptly is destroyed, the information is not entered into a system of records and a Privacy Act advisory statement is not required under 5 U.S.C. § 552a(e)(3) and DoD 5400.11-R.

If any information about an individual is maintained in a system of records; i.e., kept and retrieved by an individual's personal identifier, then a Privacy Act advisory statement is required. The individual must be told the authority that permits the agency to collect the information, whether it is mandatory to provide the information, the purposes and routine uses of the information, and the effects, if any, on the individual for not providing the information. Also, if the Social Security number (SSN) is requested, the individual must be told the federal statute or executive order of the President that allows solicitation of the SSN, whether it is mandatory to provide it, and the uses to be made of it.

For both the SSN and the other information about the individual, it will be voluntary for the individual to provide them, and the effects of not providing either may result in a delay or inability in providing information to the individual. The SSN will be used to retrieve information about the individual and to verify the individual's identity. The remaining items of the Privacy Act advisory statement (authority, purposes, and routine uses) must be derived from the component's recruiting system of records notice as published in the Federal Register.

21. INFORMATION REQUESTED IN THE PUBLIC DOMAIN

DoD 5400.11-R requires giving a Privacy Act advisory statement whenever individuals are requested to supply information about themselves for a system of records; hence, the requirement is not avoided merely because the information is in the public domain or required to be disclosed under the Freedom of Information Act (FOIA). If information solicited from an individual is to be placed in a system of records, an advisory statement is necessary, regardless of whether the same information is in the public domain or would be disclosed under the FOIA.

22. IMPLICATIONS ON VARIOUS METHODS OF DISTRIBUTING LEAVE AND EARNING STATEMENTS

Three basic methods of distributing leave and earning statements (LES) in the Department of Defense are:

- a. The LES is mailed to the individual's home address;
- b. The LES is handed out by office clerical personnel, either with or without the pay check; or
- c. The LES is handed out in an envelope by office clerical personnel either with or without the pay check.

The LES contains information about individuals that is protected by the Privacy Act. Distribution may be made in any manner so long as the information is not disclosed to persons other than those that have a requirement to process the statements in the course of their official duties. Hence, any of the methods indicated would be acceptable if the procedures preclude unauthorized disclosure to individuals outside the leave and earnings system.

23. THE APPEARANCE OF THE SOCIAL SECURITY NUMBER IN THE WINDOW OF AN ENVELOPE CONTAINING RECORD INFORMATION DOES NOT CONSTITUTE A DISCLOSURE

The appearance of the Social Security number (SSN) in a window envelope does not constitute a disclosure as contemplated by the Privacy Act. Prior to delivery to the recipient, the only likely disclosure is to personnel of the postal service who handle the letter in the performance of their official duties under agreement with the Department of Defense. However, when revising formats of the document or envelope, consideration should be given to preventing the appearance of the SSN through the window of the envelope.

24. WHAT CONSTITUTES A PRIVACY ACT REQUEST FOR ACCESS OR AMENDMENT FOR PURPOSES OF COMPLIANCE WITH PROCESSING AND REPORTING REQUIREMENTS

There is no requirement in the Privacy Act that a request specify or cite that law before it is to be processed or accounted for as a Privacy Act request. As a matter of policy, only requests which specify or clearly imply that they are being made under the Privacy Act receive the formal processing required by the law and implementing regulations and are reported as "Privacy Act requests." This avoids including routine record checks and requests to modify or update data elements in the annual Privacy Act report. This policy agrees with guidance issued by the Office of Management and Budget in Circular No. A-130, 50 Fed. Reg. 52730, 52739 (December 24, 1985). However, this does not mean that requests not citing the Privacy Act should not be honored.

25. INFORMATION PERTAINING TO THIRD PARTIES MAY NOT BE PROTECTED BY THE PRIVACY ACT

An individual's record is defined as "information about an individual that is maintained by an agency," and a system of records is "a group of any records from which information is retrieved by the name . . . or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(4) and (5), respectively. Since 5 U.S.C. § 552a(e)(1) requires that agencies maintain "only such information about an individual as is relevant and necessary," all information in an individual's record must pertain to him or her. Therefore, when an individual seeks access to or a copy of records under 5 U.S.C. § 552a(d)(1), all records pertaining to him or her in systems of records must be disclosed, with certain exceptions not here germane.

A reference to subject A in a file retrieved only by subject B's identifier would not be available to subject A under the Privacy Act. However, if an indexing capability exists so that the same file also is retrieved by subject A's identifier, then subject A and B, both, would have access to the entire record. See Voelker v. Internal Revenue Service, 646 F.2d 332 (8th Cir. 1981); Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28957 (July 9, 1975).

26. DISCLOSURE OF SECURITY CLEARANCE LEVEL

If the information concerning an individual's security clearance is classified, it is protected from disclosure under the Privacy Act if the system of records has been exempted from access pursuant to 5 U.S.C. § 552a(k)(1) and it may be protected from disclosure under the Freedom of Information Act (FOIA) exemption for classified information, 5 U.S.C. § 552(b)(1). If the information is unclassified, the individual concerned will have access under the Privacy Act, but the determination as to disclosure to a third party who has submitted a FOIA request must be made under the FOIA, 5 U.S.C. § 552(b)(6). The determination would have to be made using the balancing test, balancing the public's right to know against the individual's right of privacy. See Department of the Air Force v. Rose, 425 U.S. 352, 96 S. Ct. 1592, 48 L. Ed. 2d 11 (1976).

27. PRIVACY ACT APPLICABILITY TO LEGAL MEMORANDA MAINTAINED IN A SYSTEM OF RECORDS

The Privacy Act specifically denies authority for individual access to any information compiled in reasonable anticipation of a civil action or proceeding. 5 U.S.C. § 552a(d)(5). Not only is an attorney's "work product" protected from access under the Act, but any information compiled in reasonable anticipation of a civil action or proceeding is protected. The term "civil proceeding" covers quasi-judicial and preliminary judicial steps which are the civil counterparts to criminal proceedings occurring before actual criminal litigation. Office of Management and Budget Privacy Act Guidelines, 40 Fed. Reg. 28949, 28960 (July 9, 1975). Once information is prepared in reasonable anticipation of a civil action or proceeding, subsection (d)(5) continues to protect the material regardless of whether litigation is initiated, dropped or completed.

A determination as to whether material is prepared in anticipation of a civil action or proceeding must be made on an ad hoc basis for each document in question. In making this determination, all circumstances must be considered, including intent of the author at the time a document was prepared and the presence or imminence of a civil action or proceeding. Note: This provision applies to access under the Privacy Act only and has no effect on access, if any, available under the Freedom of Information Act, 5 U.S.C. § 552, or rules of civil procedure. Further, this determination does not apply to work product not maintained in a system of records retrieved by a personal identifier.

**28. THE PRIVACY ACT DOES NOT APPLY TO FILES INDEXED BY
NON-PERSONAL IDENTIFIERS AND RETRIEVED BY MEMORY**

Labeling of files by non-personal identifiers makes access requirements of the Privacy Act inapplicable unless such files actually are retrieved on the basis of an individual identifier through a cross-reference system or some other method. The human memory alone does not constitute across-reference system.

**29. DEPERSONALIZING COMPUTER CARDS AND PRINTOUTS BEFORE
DISPOSAL**

A massive release of computer cards and printouts for disposal is not a disclosure of personal information precluded by the Privacy Act if volume of the records, coding of information in them, or some other factor renders it impossible to pinpoint any comprehensible information about a specific individual. Such computer products may be turned over to a Defense Reutilization and Marketing Office for authorized disposal by sale or recycling, without deleting names or other identifying data.

**30. NO SUPPLEMENTAL CHARGES MAY BE ASSESSED FOR UNLISTED
TELEPHONE NUMBER SERVICE ON INSTALLATIONS WHERE NO
COMMERCIAL SERVICE IS AVAILABLE**

An individual should have the opportunity to elect not to have his or her home address and telephone number listed in a base telephone directory of class B subscribers if no commercial telephone service is available. Individuals should be excused from paying an additional cost involved in maintaining an unlisted number if they comply with regulations providing for unlisted numbers.

**31. THE PRIVACY ACT GENERAL EXEMPTION DOES NOT FOLLOW THE
RECORD**

A record created and maintained in a criminal law enforcement system of records and properly exempted under the general exemption of the Privacy Act, 5 U.S.C. § 552a(j)(2), may not retain that exemption when a copy of the record is permanently filed in a system of records maintained by a

non-criminal law enforcement activity. Specifically, copies of records otherwise afforded a general exemption will lose their exempt character when permanently filed in nonexempt systems.

Invoking the general exemption should be limited to certain systems of records maintained by only Department of Defense (DoD) criminal law enforcement activities. Such activities include police efforts to prevent, control and reduce crime or to apprehend criminals and the activities of prosecutors, courts, correctional, probation, pardon or parole authorities. The general exemption is not for systems of records maintained by any other DoD activity that may have copies of reports of criminal investigations. Congress intended that only activities which perform criminal law enforcement functions are entitled to this general exemption for a record system. Merely filing a few criminal law enforcement records in one of its records systems will not entitle an activity not involved in criminal law enforcement to invoke a general exemption for the entire system.

Individuals seeking access under the Privacy Act to criminal law enforcement records in the temporary custody of a command or activity should be directed to the organization that created the records. However, any activity's files concerning adjudication or other personnel actions based on criminal law enforcement records are the records, without the general exemption, of the using activity which shall respond to all Privacy Act requests other than those seeking access to or amendment of the criminal law enforcement record.

32. THE PRIVACY ACT SYSTEM NOTICE REQUIREMENT APPLIES TO COURT-MARTIAL FILES

Procedures and policies regarding courts-martial are governed by the Uniform Code of Military Justice and the Manual for Courts-Martial. Congress recognized the unique nature of court-martial proceedings and exempted them from requirements of the Privacy Act by specifically excluding them from the definition of "agency." See 5 U.S.C. § 551(1)(F). Although courts-martial, themselves, are not "agencies" for purposes of the Privacy Act, records of trials by courts-martial are maintained by agencies long after the courts-martial involved have been dissolved. The Privacy Act requires each agency that maintains a system of records to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records . . ." 5 U.S.C. § 552a(e)(4). Hence, the requirement to publish a system notice applies to systems containing courts-martial records.

33. A ROUTINE USE IS NOT REQUIRED FOR DISCLOSURE OF DEPARTMENT OF DEFENSE RECORDS TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION AND TO THE GENERAL SERVICES ADMINISTRATION

The Federal Records Act of 1950, as amended by the National Archives and Records Administration Act of 1984, Pub. L. 98-497, implemented by 36 C.F.R. Ch. XII and 41 C.F.R. Ch. 201, does not require a routine use notice for disclosure from Department of Defense (DoD) records systems. Such disclosures fall into three categories.

a. Records warranting permanent preservation for their historical or other value may be disclosed to the Archivist of the United States, or his representative, under the Privacy Act. See 5 U.S.C. § 552a(b)(6). Ownership of such records also may be transferred to the National Archives and Records Administration (NARA).

b. Records may be transferred to the various Federal Records Centers operated by NARA for temporary storage under the Privacy Act since such records continue to be maintained by the agency. See 5 U.S.C. § 552a(b)(1).

c. Records may be disclosed to the Archivist of the United States or the Administrator, General Services Administration, or their designees, to carry out records management inspections required by law. Such disclosures are authorized by the National Archives and Records Act of 1984. See 44 U.S.C. § 2904 and § 2906, as amended.

34. **DEFINITION OF "ORDER OF A COURT OF COMPETENT JURISDICTION"**

A subpoena signed by a clerk of a Federal or State court, without specific approval of the court itself, does not comprise an "order of a court of competent jurisdiction" for purposes of nonconsensual disclosures under the Privacy Act, 5 U.S.C. § 552a(b)(11). The overall scheme of the Privacy Act's nonconsensual disclosure provisions in subsection (b) is to balance the need for disclosure against the potential harm to the subject of the disclosure. Even though a subpoena signed by a clerk of the court is issued in the name of the court and carries with it the threat of contempt to those who ignore it, there is no guarantee that it is based upon a careful consideration of the competing interests of the litigant and the individual who is the subject of the record. It is common practice for a subpoena to be issued in blank by a court clerk to a party requesting it, who then fills in the blanks as he or she chooses.

To allow nonconsensual disclosure pursuant to a subpoena--grand jury or otherwise--would permit disclosure of protected records at the whim of any litigant, whether prosecutor, criminal defendant, or civil litigant. Therefore, disclosure of records under subsection (b)(11) requires that the court specifically order disclosure. If there is a threat of punishment for contempt for ignoring a subpoena not approved by the court, the subpoena should be challenged by a motion to quash or modify.

35. **RECORDS MAY BE DISCLOSED TO SERVICE-ORIENTED SOCIAL WELFARE ORGANIZATIONS PURSUANT TO AN ESTABLISHED ROUTINE USE**

Disclosure of personal information from records systems to service-oriented social welfare organizations, such as Army Emergency Relief, Navy Relief, Air Force Aid Society, American Red Cross, United Services Organization, etc., is permitted pursuant to properly established routine uses. See 5 U.S.C. § 552a(a)(7), (b)(3), and (e)(4)(D). However, only such information as is necessary for the welfare agency to perform its authorized functions should be provided. Information can be disclosed only if the agency which receives it adequately prevents its disclosure to persons other than their employees who need such information to perform their authorized duties.

36. PRIVACY ACT WARNING LABELS

Using warning labels indicating that particular records are subject to the Privacy Act and require protection from unauthorized disclosure should be left to the discretion of each Department of Defense (DoD) component. In accordance with 5 U.S.C. § 552a(e)(10), agencies are required to establish appropriate safeguards for records and warning labels likely would be appropriate in many cases. However, no standard warning label produced within or outside the DoD appears to be entirely satisfactory for all DoD components in all cases. Therefore, each component in its discretion may adopt existing labels or design its own labels and prescribe their internal use.

37. DISCLOSURE OF RECORDS CONCERNING CHARITABLE CONTRIBUTIONS OR PARTICIPATION IN SAVINGS BOND PROGRAMS

Disclosure of information contained in systems of records concerning employees' or service members' participation in charitable or savings bond campaigns may be necessary to those officers and employees of the Department of Defense components maintaining the systems of records who have a need for the information in the performance of their duties. 5 U.S.C. § 552a(b)(1). Disclosure under subsection (b)(1) is based on a "need-to-know" concept; consequently, disclosure would be authorized to those personnel requiring the information to discharge their duties, such as payroll and allotment clerks, key persons, and campaign aides who assist directly in implementation of the campaign. Disclosure to supervisors is neither related directly to any campaign requirement nor consistent with disclosure provisions of the Privacy Act. Disclosure should be restricted to personnel with a direct functional relationship to a campaign and for campaign purposes only. Personnel authorized to receive this information should be briefed on their responsibilities under the Privacy Act and warned against unauthorized disclosure.

38. PERSONAL NOTES AS RECORDS WITHIN A SYSTEM OF RECORDS

Personal notes of unit leaders or office supervisors concerning subordinates ordinarily are not records within a system of records governed by the Privacy Act. The Act defines "system of records" as "a group of any records under the control of any agency . . . from which information is retrieved by the . . . [individual's] identifying particular . . ." 5 U.S.C. § 552a(a)(5). One reason for limiting the definition to records "under the control of any agency" was to distinguish agency records from personal notes maintained by employees and officials of the agency. Personal notes that are merely an extension of the author's memory, if maintained properly, will not come under the provisions of the Privacy Act or the Freedom of Information Act (FOIA), 5 U.S.C. § 552.

To avoid being considered agency records, personal notes must meet certain requirements. Keeping or destroying the notes must be at the sole discretion of the author. Any requirement by superior authority, whether by oral or written directive, regulation or command policy, likely would cause the notes to

become official agency records. Such notes must be restricted to the author's personal use as memory aids. Passing them to a successor or showing them to other agency personnel would cause them to become agency records. Chapman v. National Aeronautics and Space Administration, 682 F.2d 526 (5th Cir. 1982).

Even if personal notes do become agency records, they will not be within a system of records and subject to the Privacy Act unless they are retrieved by the individual's name or other identifying particular. Thus if they are filed only under the matter in which the subordinate acted or in a chronological record of office activities, the Privacy Act would not apply to them. However, they likely would be subject to disclosure to a person requesting them under the FOIA. Individuals who maintain personal notes about agency personnel should ensure their notes do not become records within systems of records. Maintaining a system of records without complying with the Privacy Act system notice requirement could subject the individual to criminal charges and a \$5,000 fine. 5 U.S.C. § 552a(i)(2).

39. REQUIREMENT FOR PRIVACY ACT ADVISORY STATEMENTS FOR ADMINISTRATIVE PROCEEDINGS

Individuals from whom information about them is solicited during administrative proceedings must be provided Privacy Act advisory statements if records of the proceedings will be retrieved by their personal identifiers. 5 U.S.C. § 552a(e)(3).

40. ACCESS TO MEDICAL RECORDS BY INDIVIDUALS WHO COULD BE ADVERSELY AFFECTED

An individual must be given access to his or her medical and psychological records unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. That determination normally should be made in consultation with a medical doctor. When it is determined that disclosure of medical information could have an adverse effect upon the individual to whom it pertains, the information should be transmitted to a physician named by the individual and not directly to the individual. However, the physician should not be required to request the record on behalf of the individual. Information which may be harmful to the record subject should not be released to a designated individual unless the designee is qualified to make psychiatric or medical determinations. If the record subject refuses to provide a qualified designee, the request for the medical records should not be honored.

41. NO REQUIREMENT TO PROVIDE PRIVACY ACT ADVISORY STATEMENTS TO LABOR ORGANIZATIONS

A labor organization may furnish information obtained from its members to a Department of Defense (DoD) component to facilitate allotment of union dues, even though the employee-union member is not given a Privacy Act advisory statement before providing the information to the labor organization.

The Privacy Act, 5 U.S.C. § 552a, does not apply to labor organizations; hence, they are not obligated to meet the subsection (e)(3) requirement to provide Privacy Act advice to federal employees before obtaining information for a voluntary allotment of union dues. Any use of the Privacy Act advisory statement by a labor organization is voluntary and may result from express agreement with a DoD component or as a spontaneous union practice. The Standard Form 1187 used to authorize allotments from pay is required by the employee's finance office and information provided on the form will become part of a system of records from which information is retrieved using personal identifiers. If the employee furnishes the completed form to the DoD component, a Privacy Act advisory statement must be provided to the employee by the component. If the labor organization furnishes the completed form to the DoD component, no Privacy Act advisory statement is required unless the component and the labor organization have agreed otherwise.

42. INFORMATION ON FORMS ATTACHED TO SECURITY CONTAINERS OR FACILITIES IS SUBJECT TO THE PRIVACY ACT

Information consisting of names, home addresses and telephone numbers of persons designated as custodians of security storage containers or facilities, when contained in a system of records, is protected by the Privacy Act. Solicitation of such information is necessary to accomplish official Department of Defense (DoD) duties relating to protection of information stored in the containers or facilities, but it requires providing a Privacy Act advisory statement to individuals from whom and when the information is solicited. 5 U.S.C. § 552a(e)(3). This information, when appended to the exterior of a storage facility or container, is observable by any passer-by who may not be an officer or employee officially concerned with the activity. 5 U.S.C. § 552a(b)(1). Therefore, it is a disclosure subject to disclosure accounting requirements of the Act. 5 U.S.C. § 552a(c)(1). Such an accounting, however, would be impossible because of the difficulty of identifying all viewers.

The General Services Administration (GSA) has recognized that this information is subject to the Privacy Act and has revised Optional Form 63 to include a Privacy Act advisory statement and to instruct that the form be attached to the interiors of safes. When such a tag is placed inside a safe, the disclosure is limited to those officers and employees who have a need-to-know and a disclosure accounting is not required. 5 U.S.C. § 552a(b)(1) and (c)(1).

Alternatives to the disclosure accounting requirements when the information is to be displayed outside the security container or facility are:

- a. Request the individual's prior written consent for a single particular transaction; i.e., consent to disclosure of name, home address and telephone number for a particular safe, or
- b. Require notification of appropriate duty personnel with access to a control roster containing the custodians' information so they may be contacted in the case of a security problem.

43. VERIFYING THE ACCURACY OF PERSONAL DATA IN A RECORD IS SUBJECT TO THE PRIVACY ACT

Requesting an individual to verify or certify the accuracy of information about him or her in a record or on a form constitutes collection of information about the individual and is subject to advice requirements of the Privacy Act, 5 U.S.C. § 552a(e)(3). Guidance on implementation of this subsection issued by the Office of Management and Budget supports this conclusion. Subsection (e)(3) is intended "to assure that individuals from whom information about themselves is collected are informed of the reasons for requesting the information, how it may be used, and what the consequences are, if any, of not providing the information." 40 Fed. Reg. 28961 (July 9, 1975).

Either of the following situations would invoke provisions of the Privacy Act:

a. Verifying a record requires the individual to examine and disclose whether the record is correct; thus, a request for verification is a request for the individual to republish as truthful the information about him or her; or

b. The individual is asked to identify any erroneous entries and furnish the correct data. When the request is soliciting corrections or additions to a record, it is soliciting information about the individual for a system of records.

44. ONE DEPARTMENT OF DEFENSE COMPONENT MAY DISCLOSE HEALTH CARE RECORDS TO ANOTHER WITHOUT A ROUTINE USE OR CONSENT

A record may be disclosed, without the record subject's consent and without a disclosure accounting, to those officers and employees of an agency who need the records in the performance of their official duties. 5 U.S.C. § 552a(b)(1). Since the Department of Defense (DoD) is considered a single agency within the meaning of subsection (b)(1), one component's health care records may be disclosed to another in connection with valid medical research programs under the authority of this subsection.

45. DISCLOSURE OF THE ORIGINAL, PRE-1968, SERIAL NUMBER (SERVICE NUMBER) ASSIGNED TO MILITARY PERSONNEL

The original serial number, later called the service number, which military services assigned to military personnel until 1968 when it was replaced by the Social Security number (SSN), does not constitute information which cannot be disclosed to third parties. The old serial/service number did not have the same significance or importance as the SSN. The serial/service number, in and of itself, is no longer a personal identifier. Unlike the SSN, it cannot be used to facilitate linkage, consolidation, or exchange of information about an individual through multiple data banks, even within the Department of Defense (DoD). Therefore, disclosure may be made of orders and similar documents which comprise listings of names and serial/service numbers without expunging such numbers, with no invasion of personal privacy. The old serial/service number should not be confused with the SSN which can unlock innumerable data bases and provide access to much information about the individual, both inside and outside DoD.

46. THE SOCIAL SECURITY NUMBER ON BUILDING AND INSTALLATION BADGES

A Social Security number (SSN) on a building or identification badge required to be prominently displayed or worn at all times by an individual constitutes information about the individual under the Privacy Act. The SSN, with an individual's name, is a record. 5 U.S.C. § 552a(a)(4). This information, when displayed on an exposed identification badge, is observable by any passer-by who may not be an officer or employee officially concerned with the intended use of the badge. It amounts to a constant verification by the individual that information about him or her being displayed is true. Therefore, unless the SSN on a building pass or identification badge is essential, it should not be included when such passes or badges are issued, reissued, or replaced.

47. USING BOTH GENERAL AND SPECIFIC PRIVACY ACT EXEMPTIONS FOR THE SAME SYSTEM OF RECORDS

The general exemption, 5 U.S.C. § 552a(j)(2), and the specific exemption, 5 U.S.C. § 552a(k)(2), ordinarily cannot be used for the same system of records. For example, subsection (j)(2) applies to law enforcement records of criminal law enforcement activities, whereas subsection (k)(2) applies to law enforcement records other than those covered by subsection (j)(2). Nonetheless, a single system of records maintained by a law enforcement activity may contain both criminal law enforcement records exempted under (j)(2) and personnel security records exempted under (k)(5). If the two types of records are clearly segregable within the single system of records, both exemptions would apply. Also, a system of records may qualify for exemption under more than one specific exemption under subsection (k). For any system of records, only exemptions established in accordance with DoD 5400.11-R may be claimed.

48. **DISCLOSURE OF INFORMATION IN BLANKET ORDERS**

Prior to implementation of the Privacy Act on September 27, 1975, some components issued single blanket orders or other official documents concerning such personnel actions as promotions, discharges, temporary duty orders, permanent change of station orders, etc. Those documents contained limited amounts of information about each of the individuals named in them, such as Social Security numbers, homes of record, home addresses, etc. Nevertheless, disclosure of the documents to the individuals named in them is not prohibited by the Privacy Act as long as:

- a. The documents are filed in their official personnel records;
- b. The documents previously were furnished to the named individuals; and
- c. The documents were created prior to September 27, 1975.

Nothing in this advisory opinion should be construed as limiting access by an individual to third party information required to be disclosed under the Freedom of Information Act, 5 U.S.C. § 552. See 5 U.S.C. § 552a(b)(2).