DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

MCO P5211.2B
ARAD
4 Sep 97

MARINE CORPS ORDER P5211.2B

From: Commandant of the Marine Corps
To: Distribution List

Subj: THE PRIVACY ACT OF 1974

Ref: (a) SECNAVINST 5211.5D of 17 Jul 1992

Encl: (1) LOCATOR SHEET

Report Required: Privacy Act Report (Report Control DD-5211-01) (External Report Control Synbol DA&M(A) 1379 (5211)), par. 3a and chapter 12)

1. Purpose. To outline policies, conditions, and procedures governing the collection, safeguarding, maintenance, use, access, amendment, and dissemination of personal information in systems of records kept by the Marine Corps.

2. Cancellation. MCO P5211.2A.

3. Action

a. Marine Corps Activities. All Marine Corps activities shall carry out the provisions of the Privacy Act per the reference and this Manual.

b. Privacy Act Report. Commanding generals; commanding officers of Marine Corps districts; commanding; commanding officers and officers in charge not in the administrative chain of command of commanding generals and commanding officers of Marine Corps districts; and staff agencies of Headquarters, U.S. Marine Corps, shall submit an annual report of Privacy Act activities to the Commandant of the Marine Corps (ARAD) by 1 February each year. This report will cover activities occurring during the preceding calendar year. Statistical data shall be collected during the calendar year to complete this report. Refer to chapter 12 for further instructions.

4. Summary of Revision. This Manual is published incorporating previous changes that are still in effect and only minor changes for clarification of text. Chapter 11, which lists Marine Corps forms subject to the Privacy Act was deleted since forms may be frequently added, modified, or deleted.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is limited.

5. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve.

6. Certification. Reviewed and approved this date.

DISTRIBUTION: PCN 10207495000
Copy to: 7000110 (55)
8145005 (2)
7000144/8145001 (1)
70000093(2)

LOCATOR SHEET

Subj: THE PRIVACY ACT OF 1974

Location:_____
(Indicate the location(s) of the copy(ies) of this Manual.)

ENCLOSURE (1)

THE PRIVACY ACT OF 1974

RECORD OF CHANGES

Change Number	Date of Change	Date Entered	By Whom Entered

THE PRIVACY ACT OF 1974

CONTENTS

THE PRIVACY ACT OF 1974

CHAPTER 1

BACKGROUND, APPLICABILITY, AND EFFECT

THE PRIVACY ACT OF 1974

CHAPTER 1

BACKGROUND, APPLICABILITY, AND EFFECT

1000. BACKGROUND. The Privacy Act was established to give a greater control of the way records about an individual are maintained and to eliminate needless intrusions of personal privacy through the maintenance

of records. The Privacy Act is applicable to all systems of records from which information may be retrieved by name of the individual, by some identifying number, symbol, or other identifying particular assigned to or associated with an individual. The Act was designed to ensure that:

a. no Federal Government personal recordkeeping systems or files exist that are secret;

b. Federal Government personal information files are limited to which are clearly necessary;

c. individuals have an opportunity to see what information about them is maintained and to challenge its accuracy, relevancy, timeliness, and completeness;

d. personal information collected may be used only for authorized purposes unless the individual consents to other uses.

1001. APPLICABILITY AND EFFECT

1. Scope. This Manual applies to all Marine Corps military and civilian personnel including nonappropriated funded employees, and to any contractor maintaining a system of records to accomplish a Marine Corps mission. For the purposes of criminal liabilities adjudged, any contractor and employee of such contractor shall be considered an employee of the Marine Corps. This Manual applies to all requests made by individuals under the Privacy Act, for copies or review of records pertaining to themselves, that are located in a system of records subject to the Privacy Act. Additionally, all requests by individuals for records, located in a system of records, pertaining to themselves that specify the Freedom of Information Act or Privacy Act (but not both) shall be treated under the procedures established under the Act specified in the request. When the request specifies that it be processed under both the Freedom of Information Act and Privacy Act, Privacy Act procedures should be employed. The individual should be advised that the Marine Corps has elected to process the individual's request under the provisions of the Privacy Act and that all information will be provided that can be released under either the Freedom of Information Act or Privacy Act. In the event of a conflict, this Manual takes precedence over any existing Marine Corps directive dealing with the collection, maintenance, use, and dissemination of personal information.

2. Judicial Sanctions. Any member or employee of the Marine Corps may be found guilty of a misdemeanor and fined not more than $5,000 for willfully maintaining a system of records without first meeting public notice requirements; disclosing information protected under the Privacy Act to any unauthorized person or agency; or obtaining or disclosing information

about an individual under false pretenses.

3. Relationship Between the Freedom of Information Act and the Privacy Act

a. The Freedom of Information Act enables members of the public to obtain releasable records on the operation and activities of the Executive Branch of the Federal Government. The maximum amount of requested information is made available to the public unless it fails within the nine exempted categories (see MCO P5720.56).

b. The Privacy Act provides safeguards for individuals against invasions of privacy as a result of the collection of personal information by the Executive Branch of the Federal Government. The Privacy Act allows the individual of record the opportunity to request access, notification, and amendment of the personal record.

c. Exemption (b)(6) of the Freedom of Information Act ensures that there is no conflict with the Privacy Act and may be claimed when members of the public request personal records on individuals. This exemption protects the privacy of the individual from unwarranted injury, annoyance of publicity due to the release of personal records (e.g., medical or personnel files).

THE PRIVACY ACT OF 1974

CHAPTER 2

DEFINITIONS

CHAPTER 2

DEFINITIONS

2000. ACCESS. The process whereby an individual, or a representative designated by the individual, or the individual’s legal guardian, may

review or obtain copies of a record containing personal information on that individual which is in a system of records maintained by the Marine Corps.

2001. AGENCY. For purposes of disclosing records, the Department of Defense is an "agency." For all other purposes, including applications or access, appeals from denials, exempting systems of records, etc., the Marine Corps is the "agency."

2002. AMENDMENT. The modification of a record because of its inaccuracy or incompleteness.

2003. CONFIDENTIAL SOURCES. An individual or organization that has furnished information to the Federal Government under an: express promise that the identity of the source would be withheld; or implied promise to withhold the identity of the source made prior to 27 September 1975.

2004. DEFENSE DATA INTEGRITY BOARD. A Board consisting of members of the Defense Privacy Board and the DoD Inspector General or the designee, that convene to oversee, coordinate, and approve or disapprove all DoD component computer matching covered by the Privacy Act.

2005. DENIAL AUTHORITY. An official in the Marine Corps authorized either by the Secretary of the Navy or the Commandant of the Marine Corps to deny an individual’s request for notification, access of amendment when the request is made under the provisions of the Privacy Act.

2006. DISCLOSURE. The conveyance of any information from an individual’s record by any means of communication to another individual or organization. In the context of the Privacy Act and this Manual, this term only applies to personal information that is part of a system of records.

2007. EXEMPT SYSTEMS. Systems of records exempted from certain provisions of the Privacy Act because of the nature of information contained therein; e.g., classified material, information maintained in the interest of national security, certain investigative material, or test material.

2008. FEDERAL REGISTER. A publication of the U.S. Government printed for the public five times a week. It contains all current Presidential proclamations, executive orders, and regulations of Federal agencies having applicability to and legal effect on the public. It is used to publicize system notices.

2009. INDIVIDUAL. A living citizen of the United States, or an alien lawfully admitted for permanent residence, or an enlistee in the United States naval service, including a minor. Additionally, the legal guardian of an individual or a parent of a minor has the same rights as the individual, and may act on behalf of the individual concerned under the provisions of this Manual. Members of the naval service, once properly

accepted, are not minors for the purposes of this Manual. The use of the term "individual" does not, however, vest rights in the representatives of decedents to act on behalf of the decedents under this Manual, nor does the term embrace individuals acting in an entrepreneurial capacity; e.g., sole proprietorships and partnerships.

2010. INITIAL DETERMINATION. The determination made by either a systems manager or denial authority to grant or deny an individual's request for notification, access, or amendment under the provisions of the Privacy Act.

2011. MAINTAIN. When used in the context of records on individuals, includes collect, file or store, preserve, retrieve, update or change, use, or disseminate.

2012. MINOR. 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.

2013. NOTIFICATION. The process by which an individual is informed whether or not a particular system of records in the Marine Corps contains a record pertaining to the individual.

2014. OFFICIAL USE. This term encompasses those instances in which officials and employees of the Marine Corps have demonstrated need for access to any record to complete a mission or function of the Marine Corps or which is prescribed by or authorized by a directive.

2015. PERSONAL INFORMATION. Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's education, financial transactions, medical history, and criminal or employment history.

2016. PRIVACY ACT REQUEST. A request from an individual for information about the individual concerning the existence of, access to, or amendment of records that are located in a system of records.

2017. RECORD. Any item, collection or grouping of information about an individual that is maintained by or for the Marine Corps, including personal information and which contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.

2018. REVIEW AUTHORITY. The official acting for the Secretary of the Navy who reviews an initial determination that denies a request for notification, access, or amendment.

2019. RISK ASSESSMENT. An analysis which considers information sensitivity, vulnerability, and cost to a computer facility or work processing center in safeguarding personal information processed or stored in the facility or center.

2020. ROUTINE USE. The disclosure of a record outside the Department of Defense (DoD) for use that is compatible with the purpose for which the record was collected and maintained by DoD. The routine use must be included in the published system notice for the system of records involved.

2021. STATISTICAL RECORD. A record maintained for statistical research or reporting purposes only and is not to be used in whole or in part in making any determination about an identifiable individual.

2022. SYSTEM OF RECORDS. A group of records from which information "is," as opposed to "can be," retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The capability to retrieve information personal identifiers alone does not subject a system of records to the Privacy Act and this Manual.

2023. SYSTEM MANAGER. The official who has overall responsibility for records within a particular system. System managers are indicated in the published record systems notices.

2024. 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.

2025. 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 with another individual.

2026. WORKING DAY. All days excluding Saturday, Sunday, and all legal holidays.

CHAPTER 3

RESPONSIBILITIES

THE PRIVACY ACT OF 1974

CHAPTER 3

RESPONSIBILITIES

3000. RESPONSIBILITIES

1. The Commandant of the Marine Corps. The Commandant of the Marine Corps is responsible for the administration and supervision of the Privacy Act within the Marine Corps.

2. Director of Administration and Resource Management (CMC (AR)). The Director of Administration and Resource Management is designated the Principal Privacy Act Coordinator for the Marine Corps.

3. Field Commanders. Commanding generals, commanding officers of Marine Corps districts, and the commanding officers and officers in charge not in the administrative chain of command of commanding generals and district directors are responsible for implementing the contents of this Manual within their commands. To assist in the management of the Act, Privacy Act coordinators will be designated, in writing, within their respective commands. Privacy Act coordinators may be designated at subordinate levels as necessary to accomplish the purposes and requirements set forth in this Manual.

4. Denial Authority. The Commandant of the Marine Corps is the principal denial authority within the Marine Corps. The Commandant further delegates denial authority to the following officials and their deputies, assistants, or designees when requests relate to matters within their commands or areas of staff responsibility:

a. Field Activities

Commanding generals

Commanding officers, Marine Corps districts

Commanding officers, and officers in charge not in the administrative chain of command of commanding generals and district directors.

For each official listed above, their deputy or principal assistant is authorized denial authority.

b. Headquarters Marine Corps

Deputy Chief of Staff for Manpower and Reserve Affairs (CMC (M&RA))

Deputy Chief of Staff for Installations and Logistics (CMC (L))

Deputy Chief of Staff of Plans, Plans, Polices and Operations (CMC (P))

Deputy Chief of Staff for Aviation (CMC (A))

Deputy Chief of Staff for Programs and Resources (CMC (R))

Assistant Chief of Staff for Command, Control, Communications, Computer and Intelligence Department (CMC (C4I))

Staff Judge Advocate to the Commandant of the Marine Corps/Director Judge Advocate Division (CMC (JA))

Legislative Assistant to the Commandant (CMC (OLA))

Director of Public Affairs (CMC (PA))

Director of Administration and Resource Management (CMC (AR))

Director of Marine Corps History and Museums (CMC (HD))

Deputy Naval Inspector General for Marine Corps Matters/Inspector General of the Marine Corps (CMC (IG))

Counsel for the Commandant (CMC (CL))

Director, Personnel Management Division (CMC (MM))

Director, Manpower Plans and Policy Division (CMC (MP))

Director, Human Resources Division (CMC MH))

Director, Manpower Management Information Systems Division (CMC MI))

Director, Morale, Welfare and Recreation Support Activity (CMC (MW))

For each official listed above, their deputy or principal assistance is authorized denial authority.

5. Privacy Act Coordinators. Duties of the Privacy Act (PA) coordinators are as follows:

a. Serve as the primary point of contact for administration of the privacy program within their respective organizations.

b. Issue implementing instructions which designates the activity's PA coordinator, PA systems of records under their cognizance, and training aid for those personnel involved with systems of records.

c. Maintain liaison with other records management officials on matters relating to this Manual.

d. Compile and submit the annual report.

e. Review internal directives, practices, procedures, and forms for conformity with this Manual. Issue necessary supplements to this Manual.

f. Review requests for nonroutine personal data and provide an endorsement stating whether the disclosure is/is not in conflict with the Privacy Act.

6. System Managers. Duties of the system managers are:

a. Ensure that all personnel authorized access to the system or engaged in the development of procedures for handling records be informed of the requirements of the Privacy Act.

b. Determine the content and procedures for operating the system.

c. Ensure that no unpublished system of records on individuals be maintained, and that no new or significantly changed system exists without the required prepublication in the Federal Register (see chapter 9).

d. Respond to requests from individuals for information in the system. Requests for nonroutine personal data shall be referred to the local Privacy Act coordinator for review.

e. Maintain an accurate accounting of disclosures (see chapter 7).

f. Determine the relevancy and necessity of information during the development of a new system of records or when an amendment to an existing system is proposed. System managers will review the annual compilation of system notices and evaluate the following:

(1) The relationship of each time of information to the statutory or regulatory purpose for maintaining the system.

(2) The adverse consequences of not collecting each category of information.

(3) The possibility of meeting the information requirement through use of information not identifiable to the individual.

(4) Length of time the information is required.

(5) Financial cost of maintaining the data compared to the risk or adverse consequences of not maintaining.

(6) Necessity and relevance of the information to the mission of the command.

CHAPTER 4

ACCESS AND NOTIFICATION PROCEDURES

CHAPTER 4

ACCESS AND NOTIFICATION PROCEDURES

4000. PROCEDURES FOR REQUESTING ACCESS AND NOTIFICATION. The provisions of this chapter apply to requests made by individuals for access or notification of records pertaining to themselves that are contained in a system of records, even though requests specify that are made pursuant to the Freedom of Information Act. When responding, the system manager shall advise the individual which act was used to process the request and the reasons therefore. Individuals seeking access or notification should consult the systems notices published in the recent compilation in the Federal Register to identify the system(s) of records concerned and the organization/agency tasked as system manager. Individuals should then submit a request for access or notification of their record to the system manager or designated record custodian.

4001. INDIVIDUAL ACCESS TO RECORDS. Rules of access applicable to all systems of records have been established to assist the individual requesting access. Figure 4-1 illustrates the rules which a system manager should furnish the individual. It is not required that an individual be granted access to a record which is not retrievable by name or other personal identifier, except if the individual is entitled to access under the provisions of the Freedom of Information Act.

a. Initial Access or Notification Request. The request must be reasonably specific in identifying the record in a system of records. To the extent feasible, requests must include identification of system of records, and adequate personal identifiers; e.g., full name and social security number, needed to locate records in a particular system. Individuals inquiring about procedures shall be advised, when submitting requests in writing, to clearly mark the envelope and the letter "PRIVACY ACT REQUEST." In the event of possible litigation concerning a request, it is generally advisable to require an individual to make their request in writing.

b. Blanket Requests. Requests for access or notification of all systems of records within the Marine Corps shall not be honored. Individuals who make such requests shall be advised that:

(1) Requests for access or notification must be directed to the appropriate system manager for the particular record system, as indicated in the current Federal Register systems notices.

(2) Requests must either cite the particular system of records to be searched, or provide sufficient information to identify the appropriate system.

c. Verification of Identity. Prior to being given notification or

granted access to personal information, an individual shall be required by the system manager or custodian of local records to provide reasonable verification of identity. This requirement is to prevent an unwarranted disclosure to any person other than the one to whom the records or personal information pertains. Verification of identity is not required when individuals seek notification or access to records which are available to the public under the provisions of the Freedom of Information Act.

(1) Request by Mail/Other Written Form. When access or notification is requested by mail or other written form; e.g., telegram, verification of identity may be obtained by requiring the individual to provide certain minimum identifying data, such as date of birth and some item of information of the record which only the concerned individual would likely to know. If the information sought is sensitive, additional identifying data may be required. Notarized statements may not be insisted upon. The courts have ruled that an alternative method would be to have the requester provide an unsworn declaration that states, "I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct."

(2) Request in Person. In the case of an individual who seeks notification or access in person, verification of identity will normally be made from documents which the individual is likely to have readily available, such as an employee or military identification card, driver's license, or medical card.

(3) Request by Telephone. Telephone requests will not be honored.

(4) Previously Identified Record. When a record has already been identified by name or some other identifiable method, an individual shall not be denied access solely for refusing to disclose personal identifiers; e.g., social security number.

4002. TIME REQUIREMENTS FOR ACKNOWLEDGEMENTS/FINAL RESPONSE

1. Acknowledgements. A request for access, notification, or amendment of a record shall be acknowledged in writing within 10 working days of receipt of the proper system manager or record custodian. The acknowledgement shall properly identify the request and advise the individual when anticipated final action will be taken on the request. If a request for access, notification, or amendment can be acted upon within 10 working days, a separate acknowledgement is not required. For requests presented in person, a written acknowledgement will be provided at the time of receipt if the request cannot be acted upon within 10 working days.

2. Final Determinations and Action. Initial requests for access, notification or amendment shall be completed, if reasonably possible, within 30 working days, the system manager or record custodian may authorize an extension of the time by giving written notice to the requester explaining the reason for the extension, and indicating the date on which a reply can be expected.

3. Response Control. Appropriate deadlines shall be assigned each request to ensure acknowledgement and final actions are completed within the required time limit cited in paragraphs 4002.1 and 4002.2. Requests shall be clearly flagged "PRIVACY ACT REQUEST" to facilitate identification of such requests.

4003. PROCEDURES FOR GRANTING AND DENYING ACCESS OR NOTIFICATION

1. Receipt of Initial Request. One of the following actions shall be taken upon receipt of a request for access or notification of records:

a. The request shall be acknowledged as required by paragraph 4002.1.

b. If the request cannot be considered because:

(1) The identity of the requester is not verified.

(2) The requester did not identity the system of records or did not furnish adequate information to locate a record within a system.

(3) The request was forwarded to an official not having custody or responsibility for granting access or notification of the record or system of records concerned.

Inform the individual of the additional information needed or the correct way of obtaining consideration of the request for access or notification. There is no requirements that an individual be given notification or access to a record that is not retrieved by name or other personal identifier.

2. Access to Entire Requested Record or Requested Notification. If it is determined that the initial request for access or notification is sufficient to locate the records and the records are not exempt, the system manager shall advise the individual, in writing of the granted access or notification. The response to the individual shall either:

a. Advise the individual that the record may be reviewed at a specified place and time, that the individual may be accompanied by person(s) of their own choosing to review the record, that the individual may be asked to furnish a written statement authorizing discussion of the individual’s record in the presence of the accompanying person(s).

b. Furnish a copy of the requested record.

3. Partial or Complete Denial of Access. If it is determined that the requested record shall be denied in part or whole, and the system manager is not the denial authority, the system manager shall forward the request,

along with a copy of the record involved, and the reason(s) for recommending denial, to the appropriate denial authority (see denial authorities listed in chapter 3).

4. Denial of Access to Record

a. If the denial authority determines that access should be granted to the entire record, the denial authority shall make it available to the requesting individual or direct the system manager to do so. Access shall be granted in the manner outlined in paragraph 4003.2

b. If the denial authority determines that access to the entire record should be denied, the denial authority shall promptly inform the individual by letter (original and one copy) of the denial and the reason(s) therefore (including any applicable exemption), and provide a brief discussion of the significant and governmental purpose(s) served by the denial. The denial letter shall inform the individual of the right to request administrative review to the designated review authority by letter within 60 calendar days to the designated review authority (see paragraph 4003.5). The individual shall also be informed that a letter requesting such a review shall contain the enclosed copy of the denial letter and a statement of the individual's reason(s) for requesting a review of the initial determination. A copy of the denial letter shall be forwarded to the Commandant of the Marine Corps (ARAD). Denial authorities shall maintain copies of all denial letters in a form suitable for rapid retrieval, periodic statistical compilation, and management review.

c. If the denial authority determines that access to only portions of the record should be denied, the denial authority shall promptly make an expurgated copy of the record available to the requesting individual. A partial denial letter shall be issued in the manner and form provided in paragraph 4003.4b, as to the portions of the records that are required to be deleted.

5. Administrative Review of Request for Access to Record

a. The Secretary of the Navy has established procedures for individuals seeking administrative review in SECNAVINST 5211.5D. Individuals seeking administrative for access to record may petition one of the following review authorities:

(1) Director, Bureau of Information Systems, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415, if the record is from a civilian official personnel folder or is contained on any other Office of Personnel Management (OPM) form.

(2) General Counsel, Department of the Navy, Washington, DC 20360-5110, if the record concerns the employment of a present or former Marine Corps civilian employee record, such as, an employee's civilian personnel file, grievance or appeal file.

(3) Judge Advocate General (Code 34), Department of the Navy, 200 Stovall Street, Alexandria, VA 22332-2400, for any other record.

b. Upon review of the record concerned, the designated review authority shall inform the individual, in writing, of the final administrative determination. The final administrative review will be completed, if practicable, within 30 working days of receipt of the request for review. The final determination and action may be as follows:

(1) If the review authority determines that access shall be granted in whole or part, access will be provided by the review authority or system manager will be directed to do so in the manner prescribed in paragraph 4003.2.

(2) If the review authority's final determination is to deny the request for access in whole or part, the individual shall be advised of the reason(s) and statutory basis for the denial, including any exemption exercised and a brief explanation of the significant and legitimate governmental purpose served by the denial. In addition, the individual shall be advised of the right to seek judicial relief in the Federal courts.

(3) If the final denial determination is based on a security classification, either in whole or part, the individual shall be apprised of the matter relating to declassification review and appeal as set forth in SECNAVINST 5720.42.

6. Denial of the Notification of Record. If it is determined that the request for notification should be denied under an exemption and the system manager is not a denial authority, forward the request to the appropriate denial authority, along with a copy of the record concerned, and any comments and recommendations. The denial authority shall take one of the following actions:

a. If the denial authority determines that no exemption is applicable or that an exemption should not be exercised, the denial authority shall provide the requested notification or direct the system manager to do so.

b. If the denial authority determines that an exemption applies and denial of the notification would serve a significant and legitimate government purpose, for example, avoid interference of an ongoing law enforcement investigation, the requesting individual shall immediately be advised by an original and one copy of a letter that no records from the system of records requested are available to the individual under the Privacy Act. The individual shall also be informed in the denial letter of the right to request an administrative review by letter, within 60 days of the denial to the Judge Advocate General (Code 34), Department of the Navy, 200 Stovall Street, Alexandria, VA 22332-2400. The individual shall further be advised that the letter requesting an administrative review should contain a copy of the enclosed denial letter and the individual's reason(s) for requesting the review.

c. A copy of the letter denying notification shall be forwarded to the Commandant of the Marine Corps (ARAD) to be maintained for rapid retrieval, periodic statistical compilation, and management evaluation.

7. Administrative Review of Request for Notification of Record. Once a request is received for review of a denial of notification, the review authority (Judge Advocate General of the Navy) shall obtain a copy of the record concerned and make a final determination. If notification is to be granted, the review authority may provide the notification or direct the system manager to do so. If the final determination is to deny notification, the individual shall be informed that there are no records in the specified system of records that are available under the Privacy Act.

4004. SPECIAL CASES

1. Availability of Record. Access to a record will not be denied because the record is not readily available; e.g., on magnetic tape.

2. Medical Records. A medical record shall not be released directly to an individual when a judgment has been made that access to such a record could have an adverse effect on the mental or physical health of the individual. This determination should be made with the consultation of a medical doctor. The individual should be asked to provide the name of a personal physician and the record shall be provided to that physician. The foregoing shall not be considered a denial of a request for access.

3. Investigative Records. Copies of investigative records compiled by an investigative organization; e.g., the Provost Marshall or Naval Criminal and Investigative Command, but in the temporary custody of another organization holding the record for disciplinary, administrative, judicial, investigative or other purposes, are the records of the originating investigative organization. Individuals seeking notification or access, or making other requests concerning such records, shall be directed to the originating organization.

4. Noninvestigative Records. Copies of noninvestigative records located in files of another agency should be directed to the originating agency for determination of release. Noninvestigative records may include copies of records from personnel and medical records. The originating agency may authorize release of records or request transfer of the record for processing. The requester shall be notified of all transfer of records to the originating agency for processing under the Privacy Act.

5. Unit Leader’s and Supervisor’s Notes. Unit leaders and supervisors may maintain personal handwritten notes or records concerning the performance of duty of their subordinates. The only basis for establishment or continuance of such information is for memory aids for incorporation into the individual’s performance evaluation. Information of this nature is not a system of records

as contemplated by the Privacy Act and shall not be disseminated or disclosed to a successor or third party unless the notes are made part of a system of records. Extreme caution shall be exercised to ensure the security and disposal of such notes.

4005. FEES

1. Fees may be charged only for the direct cost of reproduction. When the direct cost for reproduction for a single request totals less than $15, the fee shall be automatically waived. The automatic waiver provision shall not apply when one automatic waiver has been granted to an individual and a subsequent request appears to be a duplicate or extension of the original request. The fee schedule for processing Privacy Act requests is provided in figure 4-2.

2. Checks or money orders for fees charged 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 of the activity concerned.

3. Fees may not be charged or collected for the following:

a. Searching and retrieving the record.

b. Copying at the initiative of the Marine Corps without such a request from the individual.

c. Reproducing the record for the individual to review when it is the only means by which the record may be shown to the individual; e.g., when copying the record is necessary to delete information.

d. First class postage or transporting of records.

RULES OF ACCESS

1. Requests for access must be submitted in writing to:

Commandant of the Marine Corps (Indicate Office Code)
Headquarters, U.S. Marine Corps
2 Navy Annex
Washington, DC 20380-1775

or the system manager/local record manager as shown in the systems of records in the Federal Register.

2. Individuals desiring to review records pertaining to themselves are urged to submit their requests by mail or in person 10 days before the desired review date. Every effort will be made to provide access more rapidly when necessary; however, records ordinarily cannot be made available for review on the day of the request. When the request is to provide the individual's records directly to an authorized representative, other than the parent of a minor or legal guardian, a signed authorization is required, specifying the records to be released.

3. Requests must contain certain information needed to locate and identify the record; e.g., full name, social security numbers, etc.

4. Indication of when and where record may be reviewed.

5. When a request is made in person, the custodian will require presentation of identification before providing an individual access to records pertaining to that individual. Acceptable forms of identification are an identification card, base or building pass, driver's license, medical card, or similar documents.

6. When a request is made by mail or other written form, verification of identity may be obtained by requiring the individual to provide certain minimum identifying data, such as date of birth and some items of information in the record which only the concerned individual would likely know.

7. Individuals may be accompanied by a person of their own choosing when reviewing the records; however, the custodian will not discuss the record in the presence of the third person without the written authorization of the individual to whom the records pertains. The following conditions also apply:

Figure 4-1.--Rules of Access to Title Records.

a. Do not deny access to an individual who is the subject of a record solely for refusing to divulge their social security number, unless it is the only means of retrieving the record or verifying identity.

b. Do not require the individual to explain why the record is being sought under the Privacy Act.

8. When requested, copies of the record will be provided and the response may be made by mail.

9. A medical record will not be released to the individual if in the judgment of a physician, the information contained therein could have an adverse effect on the individual's physical or mental well-being. In

this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician.

10. Questions concerning these rules of access or information contained in the record should be addressed to that record's system manager as published in the Federal Register.

Figure 4-1.--Rules of Access to Title Records--Continued.

PRIVACY ACT FEE SCHEDULE

	Cost per page
Office copy and computer printout	$.10
Microform media	
Paper copy	.25
Microfiche frame	.25

NOTE: Do not add in costs of wages of person making copies.

Figure 4-2.--Fee Schedule.

CHAPTER 5

AMENDMENT PROCEDURES

THE PRIVACY ACT OF 1974

CHAPTER 5

AMENDMENT PROCEDURES

5000. REQUEST FOR AMENDMENT OF RECORDS

1. Individuals have the right to request that their records be amended by correction, deletion, or other changes. Amendments made under the Privacy Act are limited to factual matters. The Privacy Act amendment provision, therefore does not ordinarily permit correction of judgmental decisions such as evaluations and other matters of opinion expressed in efficiency reports and selection/promotion board reports. These judgmental decisions shall be challenged via the Board for Correction of Naval Records (which is authorized to make such determinations).

2. Except in instances involving correction of routine administrative changes, requests for amendment will be submitted in writing to the system manager having physical custody of then record. The request should contain sufficient information to permit identification and location of records, a description of the item or portion for which the amendment is requested, the reason the amendment is being requested, and, if available, documentary evidence supporting the requested amendment. Certain systems of records are exempt, in part, from amendment (see chapter 10 for exempt Marine Corps systems).

3. A request will not be rejected or required to be resubmitted unless additional information is essential to process it; nor will incomplete or inaccurate requests be rejected categorically. Instead, the individual will be asked to clarify the request as needed.

5001. PROCEDURES FOR GRANTING AND DENYING AMENDMENT

1. Receipt of Initial Request. Upon receipt of a request for an amendment to records, one of the following actions shall be taken:

a. The request shall be acknowledged as required by paragraph 4002.1.

b. If the request cannot be considered because:

(1) The identity of the requester is not verified.

(2) The requester did not identify the systems of records or did not furnish adequate information to locate a record within a system.

(3) The requester did not provide adequate information or documented evidence to determine whether an amendment is warranted.

(4) The request was forwarded to an official not having custody or responsibility for amending the record.

Inform the individual of the additional information needed or the correct way of obtaining consideration of the request for amendment.

2. Amendment of Record. If the system manager determines that the request for amendment is warranted, the record shall be amended accordingly and the individual promptly advised of the action taken. Attempts should be made to identify other records under the responsibility of the system manager that are affected by the amendment. Any such records identified should be amended as necessary. The system manager shall also advise previous recipients of the record of the substance of the correction.

3. Special Procedure for Amendment of Fitness Reports. Privacy Act requests for amendment of fitness reports shall be submitted to the Commandant of the Marine Corps (MMPE). See MCO 1610.11 (Performance Evaluation Appeals), for established procedures to correct fitness reports.

4. Denial of Amendment. If the system manager is a denial authority and if the request for amendment is denied, in whole or part, the requesting individual will be provided an original and one copy of the letter explaining the reasons for the denial (copy to Commandant of the Marine Corps (ARAD)). The letter shall also inform the individual of the right to request further administrative review of the matter within 120 days by petition to the appropriate official cited below:

a. Assistant Secretary of the Navy (Manpower and Reserve Affairs), Department of the Navy, Washington, DC 20350 on matters pertaining to fitness reports or performance evaluation (including proficiency and conduct marks) from a military personnel file; or

b. Director, Bureau of Manpower Information Systems, Office of Personnel Management, 1900 E Street NW, Washington, DC 20415 on matters pertaining to the civilian official personnel folder or any OPM form; or

c. General Counsel, Department of the Navy, Washington, DC 20360-5110 on matters pertaining to present or former Marine Corps civilian employment (i.e., an employee’s grievance or appeal file); or

d. Judge Advocate General (Code 34), Department of the Navy, 200 Stovall Street, Alexandria, VA 22332-2400 for any other record.

The denial authority shall further inform the individual that a letter requesting an administrative review should enclose a copy of the denial letter and a statement as to the reason(s) for seeking the review of the initial denial of the request for amendment. If the system manager is not a denial authority, forward the request to the appropriate denial authority along with a copy of the disputed record, and any comments/ recommendations concerning disposition of the record. If the denial authority determines that the request for amendment should be granted, in whole or in part, the denial authority shall inform the system manager to take the actions cited in paragraph 5001.2. If amendment is to be denied, the denial authority shall take the actions cited in this paragraph.

5002. ADMINISTRATIVE REVIEW OF REQUEST TO AMEND RECORD

1. Upon receipt of a request for review, the appropriate official shall make a final determination granting or denying the request for amendment in whole or part. The review authority shall inform the individual in writing of the final administrative determination within 30 days of receipt of the request for review. The Assistant Secretary of the Navy (Manpower and Reserve Affairs) may authorize an extension when additional time is needed for a fair and equitable review. The individual shall be informed in writing of the reason for delay and the approximate date the review will be completed.

2. If denial is warranted, the review authority shall inform the individual in writing of :

a. The final denial of the request for amendment and the reason(s) therefor.

b. The right to file with the appropriate system manager a concise statement of the individual’s reason for disagreeing with the decision of the agency. A statement of dispute must be received by the system manager within 120 days following the date of the review authority’s final determination. The statement of dispute shall be made available to anyone to whom the record is subsequently disclosed, together with a brief statement summarizing the reason the request to amend the record was refused.

c. That prior recipients of the disputed record will be provided a copy of the statement of dispute, to the extent that an accounting of disclosure is maintained.

d. The right to seek judicial review of the review authority’s denial of amendment of the record.

3. When an individual files a statement of dispute, the system manager shall clearly annotate the record so that the dispute is apparent to anyone who may subsequently access, use or disclose it. The notation itself should be integral to the record. For automated systems of records, the notation may consist of a special indicator on the entire record or on the specific part of the record of dispute.

a. The individual's statement of dispute need not be filed as an integral part of the record to which it pertains. It shall, however, be maintained in such a manner as to permit ready retrieval whenever the disputed portion of the record is to be disclosed. When information which is the subject of a statement of dispute is subsequently disclosed, system manager shall note which information is disputed, and provide a copy of the individual's statement of dispute.

b. The system manager shall provide a copy of the statement of dispute to previous recipients of the record for whom disclosure accounting have been made and advise if the statement of dispute is relevant to the disclosed information.

c. The system manager may, if deemed appropriate, include a brief summary of the reasons for not making an amendment when disclosing disputed information. Summaries normally will be limited to the reasons stated to the individual. While these summaries may be treated as a part of the individual's record, they will not be subject to the amendment procedure of this paragraph.

4. System managers shall maintain copies of all denial letters on requests for amendments in a form that is suitable for rapid retrieval, periodic statistical compilation, and management evaluation.

CHAPTER 6

COLLECTION OF PERSONAL INFORMATION

THE PRIVACY ACT OF 1974

CHAPTER 6

COLLECTION OF PERSONAL INFORMATION

6000. POLICY CONSIDERATIONS. Each Marine Corps activity that maintains a system of records shall consider the relevance of, and the necessity for, the general categories of information to be maintained. Only information relevant and necessary to accomplish a purpose or mission as required by statute or by executive order of the President should be maintained. Since information not collected on an individual cannot be misused, minimizing the amount maintained limits the collection of extraneous information. Each Marine Corps activity should formulate, as precisely as possible, the policy objective to be served by any data gathering activity before it is undertaken. The following questions shall be considered:

1. How does the information relate to the purpose (in law) for which the system is maintained?

2. What are the adverse consequences, if any, of not collecting the information?

3. Could the need be met through the use of information that is not in individually identifiable form?

4. Is it necessary to collect information on every individual or would a sampling procedure suffice?

5. At what point will the information have satisfied the purpose for which it was collected; i.e., how long is it necessary to retain the information?

6. What is the financial cost of maintaining the record as compared to the risks/adverse consequences of not maintaining it?

7. Is the information, while generally relevant and necessary to accomplish a statutory purpose, specifically relevant and necessary only in certain cases?

6001. COLLECTION OF PERSONAL INFORMATION

1. Collection Directly From the Individual. To the extent possible,

personal information contained to systems of records will be collected directly from the individual. The collection of information from third parties will be minimal to reduce the possibility of obtaining erroneous, outdated, irrelevant, or biased information. Exceptions to this policy may be made under certain circumstances, such as the following:

a. When there is a need to ensure accuracy of information supplied by an individual through verification with a third party, such as information for a security clearance.

b. When the information can only be obtained from a third party; e.g., an employee's performance in a previous job or an investigative process.

c. When obtaining the information from the individual would prevent exceptional difficulties or result in unreasonable cost.

2. Informing Individuals From Whom Information is Requested. Individuals who are asked to supply personal information about themselves for a system of records must be provided a Privacy Act Statement before information is collected. The statement should be brief and easily understandable and given regardless of the medium used in requesting the information; e.g., a blank sheet, preprinted form or interview. This statement enables the individual to make an informed decision as to whether or not to provide the information requested. Normally, there is no requirement that the individual sign to acknowledge the Privacy Act Statement. An activity may determine that a signature is required if the information is highly sensitive. Questions posed by the individual should be answered prior to collection of the information. Figure 6-1 may be used when a separate Privacy Act Statement is required. The statement must include the following:

a. The authority; i.e., statute or executive order which authorizes the solicitation.

b. The principal purpose(s) for which the information is to be used; i.e., pay entitlement, retirement eligibility, security clearance.

c. A brief summary of the routine uses to be made of the information; i.e., the specific keys in which the information will be employed as published in the Federal Register.

d. Whether disclosure is mandatory or voluntary, the possible consequences for failing to respond, and the effect of not providing the requested information.

3. Privacy Act Statement Requirement. For the purpose of determining whether a Privacy Statement is required, refer to the definition of "personal information" as cited in paragraph 2015. Generally, personal information about an individual includes, but is not limited to, information such as:

a. Financial affairs (except items such as gross salary or grade/rank).

b. Family affairs.

c. Social and recreational affairs.

d. Medical history.

e. Political history.

f. Criminal history.

g. Information that identifies, describes, or gives a basis for inferring personal characteristics, such as voice or fingerprints.

4. Location of Privacy Act Statement. The Privacy Act Statement may be provided on the same form used to collect the information or as a supplement to the form. In certain instances, the Privacy Act Statement may be posted as a public notice, sign or poster, conspicuously displayed in the area where the information is collected. This method may be used for exchanges, clubs and messes, commissaries, or issue points for clothing, weapons, etc. In all instances where the individual requests a copy of the Privacy Act Statement, a copy shall be provided for retention.

5. Identification of Privacy Act Statement Form. When a separate Privacy Act Statement form is required, the statement, shall be assigned the same identifying number as the form used to collect the information, along with the suffix, "Privacy Act Statement;" e.g., DD Form 398 - Privacy Act Statement. If no identifying number is assigned, the Privacy Act Statement shall be identified by the report control symbol or other title identifiable to the form used to collect the information. See MCO 5211.3 (Forms and Information Requirements Subject to the Privacy Act of 1974) for administrative instructions for Marine Corps sponsored forms.

6. Command Responsiblity. The command initiating or sponsoring the request for personal information is responsible for determining whether a Privacy Act Statement is required, prepared and made available as an attachment or part of the form. Information determined to be releasable under the Freedom of Information Act does not require a Privacy Act Statement (see Chapter 11).

6002. MANDATORY VS VOLUNTARY COLLECTION FROM INDIVIDUALS

1. Collection of personal information from individuals is either mandatory or voluntary. It is mandatory for the individual to furnish information required by Public Law, Presidential Executive Order, or written directives issued by the Commandant of the Marine Corps or field commanders.

2. Some information is used to ensure that an individual receives certain

rights, benefits, and privileges to which entitled; e.g., leave papers, applications for allowances, and allotment authorizations. The decision to apply for such benefits is a voluntary action on the part of an

individual. Once the decision is made to apply, execution of the related forms is mandatory. Since information determined essential for operational and administrative purpose should be specified in written directives, all other requests for personal information are considered voluntary.

6003. DETERMINING CONSEQUENCES OF REFUSAL TO PROVIDE THE REQUESTED INFORMATION

1. The agency establishing the requirement for particular form, report, survey, questionnaire, etc., must decide whether refusal to furnish the required information may result in an adverse determination about the individual's rights, benefits, or privileges.

2. It is possible for virtually any type of form or report to have a potentially adverse impact if information requested is not provided. Failure to provide information on leave requests, fitness reports, property receipts, allotment authorizations, test answer sheets, and other forms used in routine administration could result in action adverse to the individual. The loss of denial of a right, benefit, or privilege may be cited as a consequence if an individual refuses to provide mandatory information. Commanders will ensure that the individual is fully informed of the adverse action which may result if requested information is not provided, so that the individual may make a reasonable decision whether or not to provide the information.

6004. SPECIFIC INSTRUCTIONS RELATIVE TO REQUESTING AN INDIVIDUAL'S SOCIAL SECURITY NUMBER (SSN)

1. No individual may be denied any right, benefit, or privilege provided by law because the individual refuses to disclose the SSN unless disclosure is required by Federal statute or, in the case of systems of records in existence and operating before 1 January 1975, where such disclosure was required under statute or regulation adopted prior to 1 January 1975. Executive Order 9397 of 22 November 1943 authorizes the Marine Corps to use the SSN as a numerical identifier.

2. When requesting an individual's SSN, the individual must be advised of the authority, purpose, routine use, and effect of not providing their SSN. Individuals applying for enlistment or employment in the Marine Corps who refuse to disclose their SSN will not be enlisted/commissioned in the Marine Corps or hired in a civilian capacity.

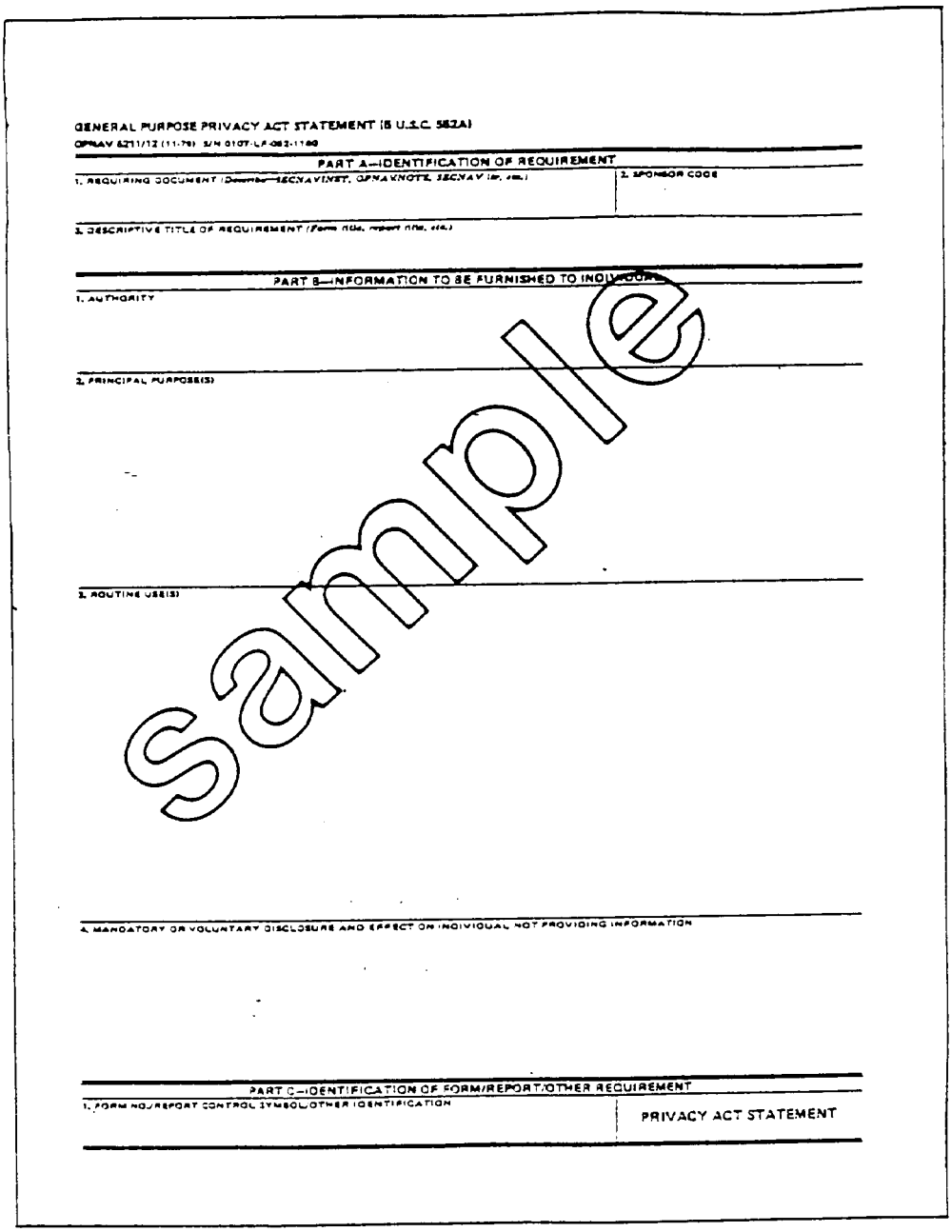
3. The individual's SSN may be requested even though it is not required by Federal statute, or is not a system of records in existence and operating

prior to 1 January 1975. A Privacy Act Statement for the SSN either separate or merged with another Privacy Act Statement, must

clearly, indicate when the SSN is not required by Federal statute and that they disclosure is voluntary. Should the individual refuse to disclose the SSN under these circumstances, the requesting activity must be prepared to identify the individual by other means.

4. Once a military member or civilian employees of the Marine Corps has disclosed their SSN for purposes of establishing personnel, financial or medical records upon entry into service or employment, the SSN becomes their identification number. It is not necessary that the individual be informed of the items of information listed in paragraph 6001.2, each time they are subsequently requested to provide or verify this identification number in connection with the aforementioned records.

6005. JAG MANUAL AND CLAIMS INVESTIGATIONS. Personal information solicited in the course of a JAG or claims investigation is subject to the provisions of the Privacy Act and this Manual. Prior to proceeding with a JAG or claims investigation, the investigating officer must consult chapters II through X and chapters II through XXIV of the JAG Manual. Liaison with the local staff judge advocate is encouraged.



GENERAL PURPOSE PRIVACY ACT STATEMENT (5 U.S.C. 552A)

OPNAV 5211/12 (11-79) S/N 0107-LF-062-1160

PART A—IDENTIFICATION OF REQUIREMENT

1. REQUIRING DOCUMENT (~~Directive~~ 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. PRINCIPAL PURPOSE(S)

3. ROUTINE USE(S)

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

PART C—IDENTIFICATION OF FORM/REPORT/OTHER REQUIREMENT

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

PRIVACY ACT STATEMENT

Figure 6-1.--General Purpose Privacy Act Statement Form.

CHAPTER 7

DISCLOSURE AND DISCLOSURE ACCOUNTING

CHAPTER 7

DISCLOSURE AND DISCLOSURE ACCOUNTING

7000. DISCLOSURE

1. General. A disclosure refers to either the transfer of a record or copy thereof, or the granting of access to a record. Except as prescribed in Chapter 4, this Manual does not authorize or compel disclosure of records to anyone other than the individual to whom the record pertains. Requests for disclosure of personal information about someone other than the individual of record shall be processed under the Freedom of Information Act (refer to MCO P5720.56).

2. Conditions of Disclosure. No record contained in a system of records shall be disclosed by any means of communication without the express written consent of the individual to whom the record pertains. Disclosure to other parties on the basis of a written consent of the individual is permitted. If the subject of the record is mentally incompetent, insane, or deceased, no medical record shall be disclosed except pursuant to a written request by or with the written request of the subject’s next of kin or legal representative. Disclosure may not be made of any record to a third party,

in the absence of a written consent, unless disclosure of the record is authorized under one or more of the conditions cited below:

a. DoD Personnel. Disclosures may be made to DoD officials and employees in the performance of their duties who have a need to know. The individual releasing the record must ensure that the DoD official or employee has a legitimate need for the requested information prior to disclosure. This includes private contractors of the DoD engaged to perform services which involve a system of records. This provision also includes transfer of records between Naval components and non-DoD agencies in connection with the Personnel Exchange Program, and interagency support agreements. While the latter transfers meet the criteria for both interagency disclosure and routine use, disclosure accounting is not required as stated in paragraph 7001.

b. Freedom of Information Act. Disclosure may be made of information required to be released under the Freedom of Information Act. Some examples of information that may be released on military personnel consists of: name, grade, date of rank, gross salary, duty status, past, present, and future duty stations (restricted to releasable Continental United States addresses), office phone number, combat service and dates, and decorations and medals. Some examples, of information that may be released on civilian employees consist of: name, grade, date of grade, gross salary, past, present, and future assignments (restricted to releasable Continental United States addresses), and office phone number. Rules for release of information are outlined in Chapter 11.

c. Routine Use

(1) Disclosure may be made for a "routine use" as defined in paragraph 2020 of this Manual and as described in the appropriate system of records notice published in the Federal Register. This may include, for example, disclosure to personnel managers, review boards, and investigating officers who require the information to discharge their official duties. Examples of personnel outside the Marine Corps who may be included are: Joint Chiefs of Staff, Military Entrance Processing Stations, or Office of Personnel Management, if they require the information to discharge an official duty. Disclosure accountings are required for all disclosures made under a routine use. Refer to Chapter 9 of this Manual for additional guidance on routine use disclosure.

(2) In addition to the routine uses established for each system of records, blanket routine uses, applicable to all record systems maintained within DoD, have been established. In the interest of simplicity, economy and to avoid redundancy, these blanket routine uses are published only once at the beginning of the Marine Corps' Federal Register Compilation of record systems notices rather than repeating them in every system notice. Blanket routine uses are contained in Marine Corps Bulletin 5211 series which lists the Marine Corps record systems notices.

d. Bureau of the Census. Disclosure may be made to the Bureau of Census for the purposes of planning or conducting a census or related activity authorized by law.

e. Statistical Research or Reporting. Disclosure may be made to an individual or organization which has provided adequate written assurance that the record will be used solely for statistical research or reporting purpose, provided the record is released in a form that is not individually identifiable; i.e., the identity of the individual cannot be deduced by tabulation or other methodology. The written request must state the purpose and intended use of the information. Disclosure accountings are not required when activities publish gross statistics covering a population in a system of records; e.g., statistics on employee turnover rates, military enlistment rates, and sick leave usage rates.

f. National Archives. Disclosure may be made to the National Archives when the record has sufficient historical value to warrant continued preservation by the U.S. Government. Additionally, disclosure may be made to the General Services Administration to determine whether the record has such value. Records transferred to a Federal record center for storage or safekeeping are not considered disclosure since the records remain under the control of the transferring agency. Disclosure accounting is not required for the records transfers to Federal records center; accounting is required for disclosures made to the National Archives.

g. Civil or Criminal Law Enforcement Activity

(1) Disclosure may be made to another civil or criminal law enforcement agency or instrumentality of the U.S. Government, state, or local government, if the head of the agency or instrumentality has made a written request to the activity which maintains the records, specifying the particular record desired and the law enforcement purpose for which the records is sought. The head of the agency or the instrumentality may have delegated the authority to request records to other officials in the organization. Requests by designated officials shall be honored provided satisfactory evidence of their authorization to request records is presented. Blanket requests for all records pertaining to an individual shall not be honored.

(2) A record may also be disclosed to a U.S., state, local or foreign law enforcement agency at the initiative of the activity which maintains the records when a violation of law is suspected, provided that such disclosure has been established in advance as a "blanket routine use" for the particular system of records involved and the misconduct is related to the purpose for which the records are maintained. See Marine Corps Bulletin 5211 series. When disclosure is contemplated under a "blanket routine use," care must be taken to ensure that the "blanket routine use"

applies to the particular system of records involved.

(3) Disclosure accountings are required for disclosure to civil or criminal law enforcement agencies, including disclosures pursuant to a routine use, but need not be disclosed to the individual if the law enforcement agency has requested in writing that it not be so disclosed.

(4) This subparagraph permits disclosures for law enforcement purposes to law enforcement agencies "within or under the control of the United States." Disclosure to foreign law enforcement agencies is not governed by any provision of the Privacy Act itself. However, disclosure at the request of foreign law enforcement agencies may, when appropriate, be made pursuant to established "blanket routine uses" for particular systems of records. See Marine Corps Bulletin 5211 series.

h. Emergency Conditions. Disclosure may be made under emergency conditions involving compelling circumstances affecting the health and safety of a person, provided notification of the disclosure is transmitted to the last known address of the individual to whom the record pertains. For example, an activity may disclose information from health records, when the time required to obtain the consent of the individual to whom the record pertains might result in a delay of medical treatment which could impair the health or safety of a person. In such emergency conditions, an attempt shall be made to verify the requester's and the medical facility's identities and the telephone number. If the information requested is considered appropriate and of an emergency nature, it may be provided by return call. Additionally, the individual about whom the records are disclosed need not necessarily be the individual whose health or safety is in peril; e.g., release of dental charts on several individuals to identify a person injured in an accident. Disclosure accountings are required for disclosure made under emergency conditions.

i. Comptroller General. Disclosure may be to the Comptroller General of the United States or to representatives authorized by the Comptroller General, in the course of the performance of duties of the General Accounting Office. Disclosure accountings are required for disclosures to the Comptroller General or General Accounting Office.

j. Order of a Court of Competent Jurisdiction. Disclosure may be made in response to an order of a court of competent jurisdiction. A subpoena signed by a Federal or state court is not an order of a court of competent jurisdiction for the purposes of disclosure under the Privacy Act. A court order for disclosure under the Privacy Act must be signed by a state or Federal court judge ordering the production of records. When the appropriate court order has been received, the following provisions apply:

(1) Public Court Order. When a record is disclosed under court

order and the issuance of the order is made public by the court that issued it, activities shall make reasonable efforts to notify the individual to whom the record pertains of the disclosure and the nature of the information provided. This requirement may be satisfied by notifying the individual by mail at the last known address contained in the activity records. Disclosure accounting is required for disclosure made pursuant to court orders.

(2) Court Order not Public. Upon being served with a court order which is not a matter of public record, an activity shall inquire from the court as to when the order will become public. An accounting for the disclosure shall be made at the time the activity complies with the order, but neither the identity of the party to who the disclosure was made nor the purpose of the disclosure shall be made available to the subject individual until the court order has become a matter of public record.

k. Congress and Members of Congress. Disclosure may be made to Congress, or, to the extent of matters within its jurisdiction, to any committee or subcommittee thereof, or to any joint committee of Congress or subcommittee thereof. Disclosure may not be made to Members of Congress who request information in their capacity or on behalf of a constituent, unless the following procedures are applied:

(1) Receipt of Request. Upon receipt of an oral or written request from a Member of Congress or member of the staff, the recipient should inquire as to the originator of the request. If it is determined that the subject of the record is the requester, information to answer the congressional request may be furnished without obtaining the individual's consent. If it is determined that the request did not originate with the subject of the record, the congressional office should be informed that information from the record cannot be disclosed unless the individual's consent is obtained. If the congressional office subsequently advises that a request for assistance or the written consent of the individual has been obtained, the requested information may be disclosed.

(2) Obtaining the Individual's Consent. If a question arises between the congressional office and the recipient of a congressional request as to who is to obtain the consent of an individual, the congressional office should be advised that Marine Corps policy is not to interfere with the relationship between a Member of Congress and a constituent. Upon congressional insistence that the Marine Corps obtain the individual's consent, the recipient shall attempt to contact the individual of record who will be afforded the opportunity to authorize or deny consent for release of information.

(3) Freedom of Information Act Implication. If neither the congressional office nor the Marine Corps obtains the individual's consent, only information required to be released by the Freedom of Information Act, as referred to in paragraph 7000.2b of this Manual and SECNAVINST 5720.42, should be furnished. For third party congressional requests, release of

information under the Freedom of Information Act may be an appropriate response.

(4) Third Party Request. If a congressional request is made on behalf of a third party; e.g., an individual's parent or spouse, the recipient should determine whether the individual, whose record is the subject of the request has consented to disclosure of the information. If the individual has given oral or written consent, the information can be disclosed. If the individual has not given oral or written consent, the information cannot be disclosed, and the congressional office should be so informed.

7001. DISCLOSURE TO CONTRACTORS. The disclosure of records to a contractor for use in the performance of a contract to accomplish a Marine Corps function, does not require the consent of the individual of record or disclosure accounting record. When the contractor is engaged to accomplish a function for the Marine Corps, the contractor and the contractor's employee are considered to be employees of the Marine Corps. Disclosure may be made of only that personal information needed by the contractor to perform a duty.

1. Contracts Involving Personal Information. The Marine Corps shall include, when soliciting bids, awarding, or administering contracts, terms that are necessary to incorporate the provisions of the Privacy Act when systems of records are involved.

2. Responsibility of the Contracting Officer. Contracting officers shall review the requirements of the contract and determine if there is a need for disclosure of information from an existing system of records or the requirement to design, development, or operate a system of records. If the contract involves a system of records, the solicitation shall contain a notice similar to the following:

WARNING

"This procurement action requires the contractor to do one or more of the following: Operate, use or maintain a system of records on individuals to accomplish an agency function. The Privacy Act of 1974 (P.L. 93-579; 5 USC 552a) imposes requirements on how these records are collected, maintained, used, and disclosed. Violations of the Privacy Act may result in termination of any contract resulting from this solicitation as well as imposition of criminal or civil penalties."

The Federal Acquisition Regulation, Part 24.1, Protection of Individual Privacy, should be consulted for further guidance on provisions of the Privacy Act when Government contractors are involved with personal information.

7002. DISCLOSURE ACCOUNTING

1. Accounting Responsibility. Each activity shall keep an accurate accounting of the date, nature, and purpose of each disclosure of an individual's record to a person or agency except as follows:

a. To DoD officials and employees for use in the performance of their assigned duties (see paragraph 7000.2a).

b. When the information is provided under the provisions of the Freedom of Information Act (see paragraph 7000.2b).

c. When activities publish gross statistics and no individual of the group can be identified (see paragraph 7000.2e).

Disclosure accounting is required even if consent is provided by the individual of record. Figure 7-1 lists the minimum information required and may be used when disclosure accounting is required.

2. Accuracy of Record. Prior to disclosure of a record on an individual to any person other than personnel of the agency, with a need to know, or under the provisions of the Freedom of Information Act, reasonable efforts should be made to ensure that the record is accurate, complete, timely, and relevant for Marine Corps purposes. In certain circumstances, it may be appropriate to advise the recipient that the information was accurate as of a specific date.

3. Purpose of Accounting. The purposes of the accounting requirement are to:

a. Allow individuals to determine to whom their records have been disclosed.

b. Provide a basis for subsequently advising recipients of records of any disputed or corrected information.

c. Provide an audit for subsequent review of activity compliance.

4. Methods of Accounting. In view of the variety of record systems, activities are given methods latitude in devising methods of disclosure accounting. There is no requirement that the accounting be retained on a record-by-record basis, although that frequently may be the capability to meet the above purposes.

5. Retention of Accounting Record. The record of accounting must be retained for at least 5 years after the last disclosure, or the life of the record, whichever is longer. The Privacy Act, however, does not require the retention of the record when the record could lawfully be disposed of sooner, per SECNAVINST P5212.5, Disposal of Navy and

Marine Corps Records.

6. Accounting to the Individual. Upon request from the individual of record, system manager or appropriate custodial official must make available all disclosure accounting information to that individual unless:

a. An exemption has been exercised.

b. Information has been disclosed to a court of competent jurisdiction as described in paragraph 7000.2j(2).

c. Information has been disclosed to another agency or instrumentality for law enforcement purposes as described in paragraph 7000.2g(1).

7003. DISCLOSURE TO CONSUMER REPORTING AGENCIES. Certain personal information may be disclosed to consumer reporting as defined by the Federal Claims Collection Act of 1966. Under 15 U.S.C. 1681, the following information may be disclosed to a consumer reporting agency:

a. Name, address, taxpayer social security number (SSN), and other information required to establish identity of the individual.

b. The amount, status and history of the claim.

c. The agency or program under which the claim arose.

The Federal Claims Collection Act of 1966 specifically requires that the system notice for the system of records from which the information will be disclosed indicates that the information may be disclosed to a consumer reporting agency.

7004. DISCLOSURE FOR MATCHING PROGRAMS

1. General Information. The Office of Management and Budget (OMB) has issued special guidelines to be followed in programs that match personal information in computerized data bases of two or more Federal agencies. See figure 7-2 for OMB Matching Guidelines. These guidelines are intended to strike a balance between the interest of the Government and the need to protect individual privacy expectations. These guidelines do not authorize matching programs as such and each matching program must be justified individually per OMB guidance.

2. Request for Matching Programs. All requests for matching programs, to include proposed amendments to the applicable systems notice, and analysis and proposed matching program reports should be forwarded to the Commandant of the Marine Corps (ARAD) for publication in the Federal Register. Any changes to existing matching programs shall be processed in the same manner.

3. Time Limits for Submission of Matching Reports. Documentation required

by submission of matching reports should be provided to the Commandant of the Marine Corps (ARAD) at least 60 days prior to the proposed initiation date of the matching program.

RECORD OF DISCLOSURE - PRIVACY ACT OF 1974. The attached record contains personal information concerning an individual. Its use and disclosure is governed by SECNAVINST 5211.5.
OPNAV 5211/9 (Rev. 6-82) S/N 0107-LF-052-1146

UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION FROM THIS RECORD COULD SUBJECT THE DISCLOSER TO CRIMINAL PENALTIES

1. This sheet is to remain a permanent part of the record described below.
2. An entry must be made each time the record or any information from the record is viewed by, or furnished to any person or agency, including the subject of the record.

except:
a. Disclosures to DoD or DoN personnel having a need to know in the performance of their official duties.
b. Disclosure of items listed in paragraph 7 SECNAVINST 5211.5

TITLE & DESCRIPTION OF RECORD

DATE OF DISCLOSURE	METHOD OF DISCLOSURE	PURPOSE OR AUTHORITY	NAME & ADDRESS OF PERSON OR AGENCY TO WHOM DISCLOSED, WITH SIGNATURE IF MADE IN PERSON

Figure 7-1.--Record of Disclosure.

OFFICE OF MANAGEMENT AND BUDGET

Matching Guidelines

A. PURPOSE. These guidelines supplement and shall be used in conjunction with OMB Guidelines on the Administration of the Privacy Act of 1974, issued in July 1, 1975, and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concerns expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These guidelines do not authorize activities that are not permitted by law, nor do they prohibit activities expressly required to be performed by law. Complying with these guidelines, however, does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these guidelines.

B. SCOPE. These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a) and to all matching programs:

1. Performed by a Federal agency, whether the personal records used in the match are Federal or nonfederal.

2. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any nonfederal organization.

C. EFFECTIVE DATE. These guidelines are effective on May 11, 1982.

D. DEFINITIONS. For the purposes of the Guidelines, all the terms defined in the Privacy Act of 1974 apply.

1. Personal Record. Any information pertaining to an individual that is stored in an automated system of records; for example, a data base which contains information about individuals that is retrieved by name or some other personal identifier.

2. Matching Programs. A procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of nonfederal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants. Matching programs do not include the following:

a. Matches that do not compare a substantial number of records, such as, comparison of the Department of Education's defaulted student loan data base with the OPM's federal employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

Figure 7-2.--Office of Management and Budget Matching Guidelines.

b. Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

c. Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

d. Matches done to produce aggregate statistical data without any personal identifiers.

e. Matches done to support any research or statistical project when the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

f. Matches done by an agency using its own records.

3. Matching Agency. The Federal agency which actually performs the match.

4. Source Agency. The Federal agency which discloses records from a system of records to be used in the match. Note that 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. The disclosure of records to the matching agency and any later disclosure of "hits" (by either the matching or the source agencies) must be done per the provisions of paragraph (b) of the Privacy Act.

5. Hit. The identification, through a matching program, of a specific individual.

E. GUIDELINES FOR AGENCIES PARTICIPATING IN MATCHING PROGRAMS. Agencies should acquire and disclose matching records and conduct matching programs per the provisions of this section and the Privacy Act.

1. Disclosing Personal Records for Matching Programs:

a. To Another Federal Agency. Source agencies are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure provisions when they do. Among the factors source agencies would consider are:

(1) Legal authority for the match;

(2) purpose and description of the match;

(3) description of the records to be matched;

(4) whether the record subjects have consented to the match; or whether disclosure of records for the match would be compatible with the purpose for which the records were originally collected; that is, whether disclosure under a "routine use" would be appropriate; whether the soliciting agency is seeking records for a legitimate law enforcement activity--whichever is appropriate; or any other provision of the Privacy Act under which disclosure may be made;

28

Figure 7-2.--Office of Management and Budget Matching Guidelines--Continued.

(5) description of additional information which may be subsequently disclosed in relation to "hits";

(6) subsequent actions expected of the source (for example, verification of the identity of the "hits" or followup with individuals who are "hits"); or

(7) safeguards to be afforded the records involved, including disposition.

b. If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a "routine use" (Section (b)(3) of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the Federal Register. The agency should also be sure to maintain an accounting of the disclosures pursuant to Section (c) of the Privacy Act.

c. To a Nonfederal Entity. Before disclosing records to a nonfederal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the consideration in paragraph E.1.a., also make reasonable efforts, pursuant to Section (e)(6) of the Privacy Act, to "assure that such records are accurate, complete, timely, and relevant for agency purposes."

2. Written Agreements. Before disclosing to either a Federal or nonfederal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file; for example, that the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file or files previously agreed to; that it will not be used to extract information concerning "nonhit" individuals for any purpose, and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

3. Performing Matching Programs

a. Matching agencies should maintain reasonable administrative, technical, and physical security safeguards on all files involved in the matching program.

b. Matching agencies should ensure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the Federal Register and reported to OMB and the Congress, as appropriate.

Figure 7-2.-- Office of Management and Budget Matching Guidelines-- Continued.

4. Disposition of Records

a. Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

b. Records relating to hits will be kept only so long as an investigation, either criminal or administrative, is active, and will be disposed of per the requirements of the Privacy Act and the Federal Records Schedule.

5. Publication Requirements

a. Agencies, before disclosing records outside the agency, will publish appropriate "routine use" notices in the Federal Register, if necessary.

b. If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate Federal Register notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

6. Reporting Requirements. As close to the initiation of the matching program as possible, matching agencies shall publish in the Federal Register a brief public notice describing the matching program. The notice should include:

a. The legal authority under which the match is being conducted;

b. a description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose or purposes for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

c. a complete description of the personal records to be matched, including the source or sources, system of records identifying data, date or dates and page number of the most recent Federal Register full text publication when appropriate;

d. the projected start and ending dates of the program;

e. the security safeguards to be used to protect against unauthorized access or disclosure of the personal records; and

f. plans for disposition of the source records and "hits."

7. Agencies should send a copy of this notice to the Congress and to OMB at the same time it is sent to the Federal Register.

a. Agencies should report new or altered systems of records as described in paragraph 8.5.b., as necessary.

Figure 7-2.--Office of Management and Budget Matching Guidelines--Continued.

b. Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and the Government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by paragraph (p) of the Privacy Act, or Section 3514 of Pub. L. 96-511.

8. Use of Contractors. Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contract. When contractors are used, however,

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by Federal Personnel Regulation Amendment 155 (41 CFR 1-1.337-5);

b. the terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, GSA, and the Department of Commerce;

c. the terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;

d. contractor personnel involved in the matching program shall be made explicity aware of their obligations under the Act and of these guidelines, agency rules, and any special safeguards in relation to each specific match performed; and

e. any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (5 U.S.C. 552a (b)(3)).

F. IMPLEMENTATION AND OVERSIGHT. The OMB will oversee the implementation of these guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with Section 6 of the Privacy Act.

Figure 7-2.--Office of Management and Budget Matching Guidelines--Continued.

CHAPTER 8

SAFEGUARDING PERSONAL INFORMATION

CHAPTER 8

SAFEGUARDING PERSONAL INFORMATION

8000. GENERAL. Each system manager will establish administrative, technical, and physical safeguards to protect each system of records from authorized or unintentional access, disclosure, modification, or destruction. Specific safeguards for individual systems must be tailored to the existing circumstances, with consideration given to sensitivity of the data, continuity of operations, general security of the area, cost of safeguards, etc. Enclosures (6) and (7) of the reference provides additional information for special consideration in using computerized systems of records and safeguarding records during work processing.

1. Responsibility. At every Marine Corps activity, an official shall be designated, for each record system, as having responsibility for safeguarding the information of that system. Any unauthorized disclosures or violations shall be reported to the Commandant of the Marine Corps (ARAD) immediately.

2. Minimum Requirement. Personal information will be considered in the same category as information designated "For Official Use Only." This provision is to provide reasonable safeguards to prevent inadvertent or unauthorized disclosures of record content during processing, storage, transmission, and disposal.

3. Automated Data Processing (ADP). The Director, Command, Control, Communications and Computer (C4I) Systems Division, Headquarters, U.S. Marine Corps (CMC (CC)) is responsible for determining and formulating policies and procedures, as necessary, to ensure that ADP systems containing personal information have adequate technical safeguards to protect personal privacy.

4. Contractual Requirement. When a contractor performs a recordkeeping function for the Marine Corps, the contractor and the contractor’s employees become subject to the Act. Any contract involving the maintenance of records shall include such terms as are necessary to incorporate the relevant provisions of the Privacy Act. The Federal Acquisition Regulation, Part 24.1, Protection of Individual Privacy should be consulted by contracting

officials relative to guidance concerning processing, accessing, maintaining, or disposing of personal information.

5. Disposal. Reasonable care must be taken to ensure that personal information is not subject to unauthorized disclosure during records disposal. Records may be disposed of by pulping, tearing, shredding, macerating, or burning to preclude recognition or reconstruction of personal information. Information on magnetic tapes or other magnetic medium may be disposed of by

erasing or degaussing. If contractors are hired to haul trash containing personal information, contract provisions as stated in paragraph 8000.4, should be incorporated in the contract. Legal assistance should be obtained in developing sales contract clauses that will make the Government contractor subject to the Privacy Act.

CHAPTER 9

ESTABLISHING OR AMENDING SYSTEMS OF RECORDS

THE PRIVACY ACT OF 1974

CHAPTER 9

ESTABLISHING OR AMENDING SYSTEMS OF RECORDS

9000. GENERAL. There will be no systems of records on individuals where the public is unaware of the existence of the records. The method used to publicize the existence of systems of records is the Federal Register. Not all Marine Corps activities receive the Federal Register, therefore, Marine Corps Bulletins in the 5211 series are distributed which pertain to Marine Corps personnel. Other notices are published in OPNAV Notices in the 5211 series. Systems of records containing personal information about individuals for which a published systems notice has not been published in the Federal Register are not authorized, and shall not be maintained. Individuals in violation of this policy are subject to Federal prosecution with a maximum fine of $5,000.

1. System Notice Review. All Marine Corps activities should review the record system notices annually an ensure that all record systems maintained have been described or are included in a published record system notice.

2. Report of New or Altered System of Records. A report on a proposed new or altered system of records shall be submitted to the CMC (ARAD). This report must reach CMC (ARAD) at least 90 days prior to planned implementation of the new or altered system. In the case of an automated system, the report shall be submitted at least 90 days prior to the planned date for issuance of solicitation for automatic data processing equipment or services, or associated telecommunication equipment or services. If no such solicitation is planned, then it must be submitted at least 90 days prior to the date of desired implementation. Proposed system notices for new or altered system of records require staffing to the OMB and to Congress for approval. Additionally, the system notice must be published in the Federal Register to afford the public 30 days for review and comment. The Federal Register publication will state the proposed new or altered system will be effective in 30 calendar days without further notice, unless comments are received which would result in a contrary determination. Any such determination would require republication of a revised notice; i.e., another 30 calendar days for further comment before implementation. (See procedures in paragraph 9001.)

3. Relevance and Necessity. Activities shall maintain in their systems of records only such personal information that is relevant and necessary to accomplish a purpose or mission. Authority to establish or maintain a system of records does not convey unlimited right to collect and maintain all information which may be useful or convenient to have as opposed to that which is relevant and necessary.

4. Restriction on Maintenance of Certain Records. Maintenance of a system of records describing how individuals exercise rights guaranteed by the First Amendment is prohibited unless expressly authorized by Federal statute, by the individual concerned, or unless it is pertinent to

and within the scope of an authorized law enforcement activity. The exercise of these rights includes, but is not limited to religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

5. Familiarity by Privacy Act Coordinators. The designated Privacy Act coordinator at each activity should become familiar with the system notices as they relate to the activity's files, so that inquiries citing system notices may be properly referred. Written indexes, relating published system notices to local records, may be necessary at larger activities to ensure proper and prompt routing of inquiries.

9001. PROCEDURES

1. Determination of Notice Requirements. Requests to establish or alter a system of records are required when the change or new system is not adequately described under an existing system notices published in the Federal Register. The following criteria are to be used when determining whether or not a report is required for a new or altered system:

a. A New System of Records. A proposed new system of records must be reported for publication in the Federal Register in order to notify the public of the existence of the system.

b. A Significant Change to an Existing System of Records (Altered System). A report is required for any significant change or alteration to an existing system of record, if the change falls within the following criteria:

(1) Number or Types of Individuals. Increases or changes of the number or types of individuals on whom the records are maintained requires a report. For example, if a system which only covered military personnel is expanded to cover both military and civilian personnel, a change to the existing system is required. Increases in the number of indivduals in a system which can be attributed to normal growth patterns need not be reported.

(2) Expansion of Categories of Information. The addition of a new category of records not currently described in the published system notice requires a report. For example, if an employee payroll system is expanded to include data on education and training, this would be an expansion of the categories of information maintained.

(3) Organization of Records. Altering the manner in which records are organized, indexed, or retrieved requires a report. For example, the centralization or decentralization of an organization may result in the consolidation of two or more systems or the splitting of two or more systems.

(4) Alteration of Purpose. Altering the purpose for which the information is used requires a report. For example, records currently used for historical purposes are to be used for making determination on eligibility for disability benefits.

(5) Changes in Computer Environment. Changes in equipment configuration software and/or procedures, so as to create the potential for either greater or easier access, requires a report. An example would be a conversion of a manual system to an automated system or the direct link use of terminals to new offices. The addition of peripheral devices such as tape and disc devices, card readers, printers, and similar devices to existing automated data processing system, does not require a report, as long as the system security is preserved.

2. Submission of Report. The report on a new system or altered system shall consist of a transmittal letter, narrative statement and any supporting documentation, as outlined below:

a. Transmittal Letter. This letter shall contain a statement of why action is being taken and forward the proposed system notice.

b. Narrative Statement. The statement (see figure 9-1), to be typed on plain bond paper, shall include, as a minimum the following:

(1) System Identification and Name. The system identification will be assigned based on the subject series indicated in figure 9-2. The numbering sequence will be assigned by this Headquarters where the XX is cited in the system identification series. The use of nicknames not readily comprehensible to the public, should be avoided when naming the system.

(2) Responsible Official. Indicates the name, title, address, and telephone number of the official responsible for submission of the new or altered system notice. This official will serve as a point of contact on inquiries about the content of the new or altered system notice.

(3) Purpose. Describe the purpose(s) of the system of record or the nature of changes being proposed.

(4) Authority. Cite, if possible, the specific Federal statute or Executive order, including the title, which authorizes the system of records. Whenever possible, provide the name or subject of the authority, for example 5 U.S.C. 4115, Collection of Training Information or E.O. 10450, Security Requirements for Government Employees. Consult the appropriate legal officer for assistance in determining statutory or regulatory basis for the system.

(5) Number of Individuals. Provide the actual number, if known, or an estimated number of individuals on whom records are maintained for the new or altered system.

(6) First Amendment Rights. Provide a description of any information to be kept on the exercise of an individual's first amendment rights and the basis for maintaining information on first amendment rights.

(7) Measures to Assure Information Accuracy. Describe procedures established to assure the accuracy, relevance, and completeness of information in the system.

(8) Other Measures to Assure System Security. Briefly describe steps taken to minimize the risk of unauthorized access to the system. When computer systems are involved provide the following information. Word processing and microform systems used in processing a system of records shall be described in a manner similar to the computer system:

(a) State whether the automation is done in a batch or on-line environment.

(b) Describe in general terms the physical safeguards of the computer site and state if a site risk analysis was performed. All new or altered automated data processing systems must show that a risk analysis was performed.

(c) If an on-line system is being described, state whether dial-up or hard-wired terminals are used in accessing the system via the terminal; e.g., a controlled area, key locks on hard-wired terminals or password protection for dial-up terminals.

(d) Provide the location where primary computer medial is stored. Generally, computer media is stored at a data processing installation (DPI) which in most instances is not the system location.

(e) Describe the technical procedures used to protect on-line data from unauthorized disclosures. For example, in cases where retrieval languages are part of a computer system, describe the control procedures for ensuring that the information accessed is in conformity with the published system notice.

(9) Relations to State/Local Government Activities. Discuss briefly the relationship of the system to state or local government activities as the sources or recipients of information in the system.

(10) Supporting Documentation. Submit a documentation to support the new or changed system, as follows:

(a) Provide a copy of the new system notice or change which the activity proposes to publish. Record system notices shall be written in a style understandable to the general public. Abbreviations, nicknames, or acronyms may be used if they are spelled out first; jargon and codes

shall be avoided. Figure 9-3 provides detailed instructions for preparing the system notice. Figure 9-4 is an example of a completed system notice.

(b) If applicable, include a statement concerning any proposed exemptions, citing the statutory authority for the exemption, and the reason(s) it is to be exempted from the specific provision(s).

3. Amendment of System of Records. Changes to an existing system of records that do not fall within the criteria cited in paragraph 9001.1b, shall be reported as amendments. For example, certain amendments to a published system notice may include changes in location, authority for the system, system manager, notification procedures, and claiming an exemption for an existing nonexempt system. Figure 9-5 is a sample format for an amendment to a system notice. The amendment notice shall be typed on plain bond paper. The proposed amendment should be submitted approximately 90 days before the change is to take place. The submission of an amendment notice should include the following:

a. The system identification and name; e.g., MMN00006, Military Personnel Records (OQR/SRB).

b. The specific change(s) proposed.

c. The full text of the system notice, as amended. Refer to figure 9-4 for format of a complete system notice.

4. Deletion of System Notices. System managers shall report, when necessary, any system of records which should be deleted. This includes systems of records that have been discontinued and combined with another system or determined not to be subject to the Privacy Act. Submit a brief statement to the CMC (ARAD) providing notification that the notice is not longer required and the reason.

5. Responsibility for Processing Reports on System Notices. Notices of new or changed system notices shall be submitted to the CMC (ARAD) for processing and forwarding to the Chief of Naval Operations (OP9B30), Washington, DC 20350-2000. The CMC (ARAD) shall provide assistance to activities requesting new or changed system notices.

DEPARTMENT OF DEFENSE
U.S. MARINE CORPS
Report on a New System Under the
Privacy Act of 1974

1. System Identification and Name. MMN00045 "Automated Systematic Recruiting Support System."

2. Responsible Official. Any inquiries or comments on the proposed new system notice may be directed to Mr. John Smith, Head, Automated Services Center, Marine Corps Recruit Depot/Eastern Recruiting Region, Parris Island, SC 29905-5001, telephone (803) 485-1111.

3. Purpose. To maintain a data base of all Marine Corps recruits. The system will be used in the administration of all Marine Corps recruits from entry through the completion of recruit training. The social security number is required in this system because it is a unique identifier.

4. Authority for Maintenance of the System. Enlistment Recruiting Campaigns, 10 U.S.Code 503; Department Regulations, 5 U.S. Code 301.

5. Number of Individuals. The system will effect approximately 50,000 individuals a year.

6. Information on First Amendment Activities. No information relating to an individual's exercise of first amendment rights is contained in this system.

7. Measures to Assure Information Accuracy. The accuracy of data will be checked by a series of edits built into the system's software package. All data elements are validated in accordance with established criteria at the time of data entry. Invalid items are rejected at time data is entered. On-line updating provides for subsequent changes/corrections of data.

8. Other Measures to Assure System Security

a. The system primarily operates in the on-line mode for data entry.

b. Both dial-up and hard-wired terminals support the system. System information is protected by the following software features: user account number and password sign-on, data base access authority, data set and data item authority for add, update, and delete.

c. Access to the building in which the computer system is located is protected by uniformed guards requiring positive identification for admission. Access to the terminals is under the control

Figure 9-1.--Sample Format for Report on New System.

of authorized personnel during working hours; the office space in which the terminals are located is locked after official working hours.

9. Relations to State/Local Government Activities. None.

10. Supporting Documentation. No changes to existing procedural or exemption rules are required. Enclosure (1) Advanced copy of the proposed system notice.

Figure 9-1.--Sample Format for Report on New System--Continued.

MARINE CORPS PRIVACY ACT SUBJECT SERIES
FOR SYSTEM NOTICES

SUBJECT SERIES	SYSTEM IDENTIFICATION SERIES
Aviation	MAA000XX
Fiscal/Disbursing (Matters relating to pay)	MFD000XX
Historical	MHD000XXX
Installations and Logistics	MIL000XX
Judge Advocate/Legal Matters	MJA000XX
Miscellaneous	MMC000XX
Manpower/Personnel	MMM000XX
Training	MMT000XX
Reserve	MRS000XX
Telecommunication/Telephone Billing	MTE000XX

Figure 9-2.--Subject Series for System Notices.

INSTRUCTIONS FOR PREPARATION OF SYSTEM NOTICES

System identification: The Marine Corps identifier must appear on all systems notices and shall be limited to 21 positions including any file number/symbols, punctuation, and spacing. See figure 9-2 for system

identification series. The numbering sequence indicated by X will be assigned by Headquarters Marine Corps.

System name: The official name of the system should reasonably reflect the categories of personal information in the system. In no event shall the system name exceed 55 character positions, punctuation, and spacing.

Location: If the system is maintained in a single location, provide the exact name of the office. If the system is geographically or organizationally decentralized, specify each type of organization or element that maintains a segment of the system. For example, if the system comprises clinical records, location might include medical centers and hospitals as well as the National Personnel Records Center. Where automated data systems encompass a central computer facility, with input/output terminals at several geographical locations, list locations by category. Where multiple locations are referred to by type of organization, state: "See the organizational elements of the U.S. Marine Corps as listed in the Department of the Navy Address Directory appearing in the Federal Register."

Categories of individuals covered by the system: The purpose of this requirement is to permit individuals to know whether or not information on them might be in the system of records. Description of categories, therefore, shall be stated in easily understood, nontechnical terms. Avoid using broad general descriptions such as "all military personnel," unless the system really applies to all military personnel and just to those assigned to the organization. Any change to the category of individuals which increases the number or type of individuals on whom records are maintained may require preparation and publication of a revised notice; i.e., a system which only covered military personnel is expanded to include dependents.

Categories of records in the system: Briefly describe in nontechnical terms all types of information in the system; e.g., medical history, medical treatment, clinical, employment history, applications, etc. Source documents which support automatic records will not be listed unless they are retained and filed by name, SSN, or other individual identifier. Any expansion and/or addition of categories of information maintained will require preparation and publication of revised notices; e.g., the expansion of an employee payroll file to include data on education and training.

Figure 9-3.--Instructions for Preparation of System Notices.

INSTRUCTIONS FOR PREPARATION OF SYSTEM NOTICES

Authority for maintenance of the system: Authority to maintain a system of records does not give an activity grounds for maintaining information it deems merely useful. Information in a system of records must be both relevant and necessary to its mission. Cite the specific provision of Federal statute or Executive order, including the title, which authorizes

or provides a legal basis for maintenance of the system. The authority cited should be that authorizing the program which the system of records supports and not solely relying on a general statute authorizing recordkeeping, such as 5 U.S.C. 301, Departmental Regulations. Whenever possible, cite the popular name or subject of the authority, as well as a statute, public law, U.S.C. or E.O. number; e.g., "Tea-Tasters Licensing Act of 1975, 51 U.S.C. 2103." In addition, cite the DoD Directive, Navy Instruction, or Marine Corps Order which authorizes the maintenance of the system.

Purpose(s): List the specific purpose for maintaining the system of records. List only the uses made of the information within the Marine Corps (internal routine uses).

Routine uses: The blanket routine uses listed at the beginning of each compilation in the Federal Register apply to all systems notices unless otherwise specified in a notice. An explanation of each blanket routine use is listed in figure 9-6. List only the routine uses of the information made outside the DoD.

a. If the blanket routine uses apply, make the following statement: "The blanket routine uses that appear at the beginning of this compilation apply to this system."

b. For all other routine uses, list the specific organization to which the record may be released; for example, "to the Veterans Administration, to the Department of Justice," or to "state and local health agencies." For each routine use listed, state the purpose(s) for which the record is to be released. Do not use general statements, such as "to other Federal agencies as required" or "to any other appropriate Federal agency.

Record management policies and practices: This element of the system notice shall describe how the records are maintained, how they are safeguarded, what categories of officials within the Marine Corps are permitted to have access, and how long records are retained. The element shall be subdivided into four parts as follows:

a. Storage: Indicate the medium in which the records are maintained. For example, a system may be "automated, maintained on magnetic tapes or discs", "manual", or "in paper files", or a hybrid combination of paper forms and information on discs. Storage does not refer to the container or facility in which the records are kept.

Figure 9-3.--Instructions for Preparation of System Notices.--Continued.

b. Retrievability: Specify how the records are retrieved; e.g., by name, SSN, military service number or other identification numbers, classification

or personal characteristics, such as fingerprint classification, voice print identifier, etc.

c. Safeguards: Describe the categories of the immediate official custodians having access to the system as well as the responsibility of safeguarding against unauthorized access. Specify the systems.

d. Retention and disposal: State how long records are maintained, if and when they are moved to a Federal Records Center or transferred to the National Archives, or are destroyed. Consult SECNAVINST 5212.5, Disposal of Navy and Marine Corps Records, for disposal of records.

System manager(s) and address: In all cases provide the title and business address of the official responsible for the management of the system; e.g., Commandant of the Marine Corps (ARAD), Headquarters, U.S. Marine Corps, 2 Navy Annex, Washington, DC 20380-1775. For geographically or organizationally decentralized systems where individuals may deal directly with officials at each location, give the position or duty title of each category of officials responsible for the system or a segment thereof. For example, in the case of service record book, the entries would be: "Commanding Officer of the activity to which the individual is assigned."

Notification procedures: Briefly summarize the procedures whereby an individual may make an inquiry to determine whether the system contains a record about them. At a minimum, this element should identify the official title (normally the system manager and address(es)) to which an inquiry should be directed. Specify what information is required from requesting individuals to determine whether or not the system contains a record about them, such as full name, military status, SSN or service number, date of birth, etc. Identify those offices to which the requester may write or visit to obtain information and indicate any proof of identity deemed necessary.

Record access procedures: This element shall state the procedures whereby individuals can be notified at their request how they can gain access to any category of officials who can provide assistance; otherwise, the system manager.

Contesting record procedures: This element requires informing individuals how to contest the contents of the record; i.e., "The agency's rules for contesting and appealing initial determinations by the individual concerned may be obtained from the system manager."

Figure 9-3.--Instructions for Preparation of System Notices.--Continued.

Record source categories: This element requires a listing of sources of the information; e.g., the individual's previous employers, financial institutions, educational institutions, trade associations, or automated system interfaces.

Exemptions claimed for system: If no exemption has been approved for the record system, indicate "None." If there is an exemption, indicate under which subsection(s) of the Act; e.g., (j)(2), (k)(2), or (k)(4). Refer to paragraph 10001 of this Manual for guidance on exemptions under the Privacy Act. Also cite the Marine Corps order and code Federal regulations section from the Federal Register in which the rule is contained. For example, "Parts of this record system may be exempt under Title 5 U.S.C. 552a (k)(2) and (5), as applicable. Exemption rule for the system is contained in 32 C.F.R., Part 701, Subpart E, and MCO P5211.2."

Figure 9-3.--Instructions for Preparation of System Notices.--Continued.

THE PRIVACY ACT OF 1974

SYSTEM NOTICE

MMNOOOO1

System name:

Absentee Processing and Deserter Inquiry File

System location:

Primary System - Absentee and Deserter Section, Human Resources Division (MH), Manpower Department, Headquarters, U.S. Marine Corps, 2 Navy Annex, Washington, DC 20380-1775

Decentralized Segments - U.S. Marine Corps commands to which the absentee or deserter is assigned for duty or administration of official records. See the organization elements of the U.S. Marine Corps as listed in the Directory of the Department of the Navy Mailing Addresses.

Categories of individuals covered by the system:

Marine Corps absentees and deserters; Marines in hands of civil authorities, foreign and domestic; suspected and convicted absentees and deserters who have returned to military control.

Categories of records in the system:

File contains personal identification data, parent command, notation of arrests, nature and dispositions of criminal charges, and other pertinent information which is necessary to monitor, control and identify absentees, and deserters.

Authority for maintenance of the system:

Title 10 U.S.C. 5031, Secretary of the Navy; responsibilities.

Purpose(s):

To provide a record of absentees or deserters for identification, apprehension, return to military control, or monitoring members located in a foreign country.

Figure 9-4.--Completed System Notice.

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 Marine Corps compilation apply to this system.

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

Storage: Records are stored on magnetic tapes ad discs, microform, and in file folders.

Retrievability: Records may be accessed by name and SSN.

Safeguards: Building employs security guards. Computer terminals and records are located in areas accessible only to be authorized personnel that are properly screened, cleared, and trained. Use of terminals requires knowledge of passwords.

Retention and disposal: Records vary in the period of time retained. Records on magnetic tapes and discs are destroyed by erasing after disposition of the individual's case. Paper records are maintained only as long as necessary to transfer information to the official personnel record, then they are destroyed.

System manager(s) and address:

The Commandant of the Marine Corps (MH), Headquarters, U.S. Marine Corps, 2 Navy Annex, Washington, DC 20380-1775

Record access procedures:

Requests from individuals should be addressed to: Commandant of the Marine Corps (MH), Headquarters, U.S. Marine Corps, 2 Navy Annex, Washington, DC 20380-1775

Written requests for information should contain the full name of the individual date and place of birth, SSN, and signature.

For personal visits, the individual should be able to provide military identification card, driver's license, or another type of identification

bearing picture or signature, or by providing verbal data sufficient to ensure that the individual is the subject of the record.

Figure 9-4.--Completed System Notice.--Continued.

Contesting record procedures:

The rules for contesting contents and appealing initial determination may be obtained from the system manager.

Record source categories:

Information in the system is obtained from the Marine Corps Military Personnel Records; from the individual's commanding officer, officer in charge, Federal, state, and local law enforcement agencies, lawyers, judges, Members of Congress, relatives of the individual and private citizens, the Veterans Administration and the individuals themselves.

Exemptions claimed for the system:

None.

Figure 9-4.--Completed System Notice.--Continued.

AMENDMENT OF SYSTEM NOTICE
MMN00001

System name: Deserter Inquiry File

Changes:

System name: Delete the entire entry and substitute: "Absentee Processing and Deserter File."

System location: Delete the entire entry and substitute: " - Primary System Absentee and Deserter Section, Human Resources Division (MH), Headquarters, U.S. Marine Corps, Washington, DC 20380-1775. Decentralized Segments - U.S. Marine Corps commands to which the absentee is assigned for duty or administration."

Categories of individuals covered by the system: Add the following phrase to the last sentence: "...within the last 90 days."

System manager(s) and address: Delete the third sentence and substitute: "...See the Directory of the Navy and Marine Corps Activities Mailing Addresses."

Figure 9-5.--Sample Format for Amendment of System Notice.

BLANKET ROUTINE USES

BLANKET ROUTINE USES

Certain 'blanket routine uses' of the records have been established that are applicable to every record system maintained within the Department of Defense unless specifically stated otherwise within a particular record system. These additional blanket routine uses of the records are published below only once in the interest of simplicity, economy and to avoid redundancy.

LAW ENFORCEMENT ROUTINE USE

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.

DISCLOSURE WHEN REQUESTING INFORMATION ROUTINE USE

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 or other pertinent 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.

DISCLOSURE OF REQUESTED INFORMATION ROUTINE USE

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.

CONGRESSIONAL INQUIRIES ROUTINE USE

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.

PRIVATE RELIEF LEGISLATION ROUTINE USE

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.

DISCLOSURES REQUIRED BY INTERNATIONAL AGREEMENTS ROUTINE USE

A record from a system of records maintained by this component may be

3A

Figure 9-6.--Blanket Routine Uses.

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.

DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES ROUTINE USE

Any information normally contained in IRS Form W-2 which 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 Number 76-07.

DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT ROUTINE USE

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 deductions, and any other information necessary for the Office of Personnel Management to carry out its legally authorized Government-wide personnel management functions and studies.

DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION ROUTINE USE

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.

DISCLOSURE TO MILITARY BANKING FACILITIES OVERSEAS ROUTINE USE

Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who 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 may be provided 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.

DISCLOSURE OF INFORMATION TO THE GENERAL SERVICES ADMINISTRATION ROUTINE USE

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.

Figure 9-6.--Blanket Routine Uses--Continued.

BLANKET ROUTINE USES

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

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.

DISCLOSURE TO THE MERIT SYSTEMS PROTECTION BOARD ROUTINE USE

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 and 1206, or as may be authorized by law.

COUNTERINTELLIGENCE PURPOSES ROUTINE USE

A record from a system of records maintained by this component may be disclosed as a routine use outside the DOD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

3C

Figure 9-6.--Blanket Routine Uses--Continued.

THE PRIVACY ACT OF 1974

CHAPTER 10

EXEMPTIONS

THE PRIVACY ACT OF 1974

CHAPTER 10

EXEMPTIONS

10000. GENERAL. Portions of information in certain systems of records maintained by the Department of the Navy and the Marine Corps have been exempted from provisions of the Privacy Act. Information concerning the name of the system, the provisions from which the system is exempted, and the reason(s) for exemption of the record system, are published in the Federal Register. A list of Marine Corps exempted systems of records is contained at figure 10-1. Within the Department of the Navy, only the Secretary of the Navy is authorized to exempt systems of records. No system of records is automatically exempt from all provisions of the Privacy Act.

10001. AUTHORIZED EXEMPTIONS. There are two categories of authorized exemptions:

1. General Exemption. A system of records may be granted a general exemption by the Secretary of the Navy if maintained by an activity having, as its principal function: (a) the enforcement of criminal law, including the prevention, control or reduction of crime; (b) the apprehension of criminals; and (c) the efforts of prosecutors, courts, and authorities dealing with correctional, probational, pardon, or parole matters. (Exemption (j)(2)

applies.) Additionally, to qualify for a general exemption, a records system must consist of:

a. Individual Criminal Offenders. Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and containing only identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probational status.

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

c. Enforcement of Criminal Laws. Reports identifiable to an individual compiled at any stage in the process of enforcement of criminal laws from arrest or indictment through release from supervision.

2. Specific Exemptions. The Secretary of the Navy may exempt any system of records within the Marine Corps from certain provisions of the Privacy Act if the system of records meets any of the following criteria:

a. National Security Information. Information classified in the interest of national security. Before denying an individual access to classified information, the denial authority must ensure that the information is still properly classified and that it must remain classified in the interest of national security. See paragraph 10003.1, for guidance on review of classified information. (Exemption (k)(1) applies.)

b. Investigative Records Not Claimed under the General Exemption. Investigative records compiled for law enforcement purposes other than material covered under a general exemption. If the information has been used to deny the individual a right, benefit, or privilege, the information must be provided unless releasing it would reveal a confidential source. See paragraph 10003.2, for further guidance. (Exemption (k)(2) applies.)

c. Protection for President of the United States. Records maintained in connection with providing protective services to the President of the United States or other individuals authorized such protection. (Exemption (k)(3) applies.)

d. Statistical Research. Records used only for statistical research or other evaluation purposes and which are not used to make decisions on the rights, privileges, or benefits of individuals. (Exemption (k)(4) applies.)

e. Investigative Records for Suitability of Employment. Investigative records compiled solely for the purposes of determining suitability or qualifications for Federal civilian employment, military service, Federal contracts or access to classified information, but only to the extent that providing an individual with access to such records could reveal the

identity of a confidential source. (Exemption (k)(5) applies.)

f. Test or Examination Material. Test 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. (Exemption (k)(6) applies.)

g. Promotional Evaluation Records. Evaluation records used for determining potential for promotion in the Marine Corps, but only to the extent that providing and individual with access to such records would reveal the identity of a confidential source. (Exemption (k)(7) applies.)

10002. PROMISE OF CONFIDENTIALITY. Express promises of confidentiality may be granted only in those cases in which the item to be kept confidential is filed in an exempt system of records. Denial authorities are authorized to grant expressed promises of confidentiality on a selective basis, when such promises are needed and in the best interest of the Marine Corps. Officials shall establish appropriate procedures and standards governing the granting of confidentiality for records systems under their cognizance.

10003. EXEMPTION PROCEDURES. Denial authorities are authorized to deny requests for notification, access, and amendment only when the system of records published in the Federal Register has been identified as being exempt from certain provisions of the Privacy Act and when a legitimate purpose is served by invoking the exemption.

1. Classified Exemption. Denial authorities may exercise exemptions for security reasons. However, prior to exercising this exemption the denial authority must take the following actions:

a. Security Review. Perform a security reveiw of the classified record. Denial authority having classification jurisdiction over the classified record, shall review the record as set forth in OPNAVINST 5510.1, Department of the Navy Information Security Program Regulation. If the denial authority does not have classification jurisdiction, immediate coordination with the official having such authority must be made.

b. Determination of Clearance. If as a result of a security review, it is determined that the record cannot be declassified, the security clearance of the individual must be determined with a review toward granting access to the record.

2. Law Enforcement Records. Requests for access shall not be denied on the basis of an exemption if the requested record has been used as a basis for denying the individual a right, benefit, or privilege to which the individual would be entitled in the absence of the record, except that access may be limited to the extent necessary to protect the identity of a confidential source, as defined in paragraph 10002, above or unless it would:

a. Interfere with law enforcement proceedings.

b. Deprive a person of a right to a fair trial or an impartial adjudication.

c. Constitute an unwarranted invasion of personal privacy.

d. Disclose the identity of a confidential source or disclose confidential information furnished only by a confidential source in the course of a criminal investigation or in the course of a lawful national security intelligence investigation.

e. Disclose investigative techniques and procedures not already in the public domain and requiring protection from public disclosures to ensure their effectiveness.

f. Endanger the life or physical safety of law enforcement personnel.

g. Otherwise be deemed not releasable under the Freedom of the Information Act.

THE PRIVACY ACT OF 1974

EXEMPTIONS FOR MARINE CORPS RECORDS SYSTEMS

1. ID - MMN00018

SYSNAME - Base Security Incident Reporting System

EXEMPTION - Portions of this system of records are exempt from the following subsections of Title 5, United States Code, Section 552a: (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 possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction, or fabrication 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.

2. ID - MINOOOO1

SYSNAME - Personnel Security Eligibility and Access Information System

EXEMPTION - Portions of this system of records are exempt from the following subsections of Title 5, United States Code, Section 552a: (c)(3), (d), (e)(1) through (3), (e)(4)(G) through (I), and (f).

AUTHORITY - 5 U.S.C. 552a (k)(2), (3), and (5), as applicable.

REASONS - Exempt portions of this system contain information that has been properly classified under Executive Order No. 12065, National Security Information and Material, and that is required to be kept secret in the interest of national security or foreign policy.

Figure 10-1.--Marine Corps Exemptions.

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 the individual’s identity would not be revealed to the subject of record.

Exempted portions of this system further contain information that identifies sources whose confidentiality must be protected to ensure that the privacy and physical safety of those witnesses and informants are protected.

Figure 10-1.--Marine Corps Exemptions--Continued.

CHAPTER 11

GUIDELINES FOR RELEASE OF PERSONAL INFORMATION

THE PRIVACY ACT OF 1974

CHAPTER 11

GUIDELINES FOR RELEASE OF PERSONAL INFORMATION

11000. GENERAL. The provisions of this chapter apply to all requests for personal information or assistance concerning Marine Corps military and civilian personnel.

1. Background. It is the policy of the Marine Corps, consistent with the Freedom of Information Act (FOIA) to make available to the public the maximum amount of information concerning its operations and activities (see MCO P5720.56). Exemption (b)(6) of the FOIA clearly states that the information in personnel and medical records and similar files are exempt from the provisions of the FOIA if disclosure to a member of the public would result in a clearly unwarranted invasion of an individual's privacy. This chapter provides guidance as to what personal information can or cannot be disclosed.

NOTE: To comply with the Privacy Act of 1974, any record contained in a system of records filed by name and/or other personal identifier, may not be released unless it meets one of the criteria described in chapter 7 of this Manual.

2. Guidelines for Assisting Commercial Firms. Commercial firms hold the same position and relationship to their customers and to the Government as they did prior to the enactment of the Privacy Act. This means that all banks, branch banks, military banking facilities, credit unions, or any commercial facility or concession operating on a Marine Corps installation have no better standing than any other commercial enterprise in obtaining personal information about Marine Corps personnel. The Marine Corps presumes that commercial enterprises are responsible for safeguarding the information provided by their patrons. Commercial firms may request credit information on Marine Corps personnel. Information determined to be releasable under the FOIA such as the name of employee, position/job title, grade, gross salary, dates of employment, or similar information may be provided for credit information (see figures 11-1 and 11-2). Request for particular information; for example, an evaluation of personal characteristics which may include pay habits, if known, shall not be provided unless written consent of the individual has been furnished.

a. Individual Consent. Disclosure may be made of any personal information when prior written consent for the release has been obtained from the individual concerned. There is nothing to preclude commercial enterprises in their direct bilateral negotiations from soliciting any

personal information deemed necessary. This may include information received from the individual concerned or extracted from a form incorporating a consent for disclosure of personal information. This form will be signed by their potential customers. The agreement may require

the customer to sign a consent to release personal information at time of a conditional sale, agreement, etc. Below is an example of consent and activities shall provide the appropriate information:

"I hereby authorize the Marine Corps to verify my SSN or other identifiers and disclose my home address to authorized (name of commercial firm) officials so that they may contact me in connection with my financial business with (name of commercial form)."

b. Locator Assistance. If an individual employed with the Marine Corps is reassigned and fails to inform a commercial enterprise of their whereabouts and has a financial obligation to the firm, the remedy is to seek the locator assistance of the individual's last known commander or supervisor at the official position or duty station within that particular Marine Corps activity. That commander or supervisor shall either furnish the individual's new official duty location address to the requester or forward, through official channels, any correspondence received pertaining thereto to the individual's new commander or supervisor for appropriate assistance and responses. Correspondence addressed to the individual concerned at their last official place of business or duty station will be forwarded as provided by postal regulations to the new location. Once an individual's affiliation with the Marine Corps is terminated through separation or retirement, locator assistance to provide the home address is severely curtailed unless the public interest dictates disclosure of the last known home address. The activity may at its discretion forward correspondence to the individual's last known home address. The Marine Corps, however, is not obligated to act as an intermediary for private matters concerning former Marine Corps personnel.

3. Releasable Information Under FOIA. Information which should be released under the FOIA shall be provided to the public. Verification of identity shall be required of an individual and/or commercial enterprise seeking access to information under the FOIA only when such information is relevant to determine whether a "clearly unwarranted invasion of privacy" would result. Refer to MCO P5720.56 and SECNAVINST 5720.42 for procedures in responding to FOIA requests. The following guidance is provided for use in determining what information on an individual should or should not be released to the public.

a. Exception of FOIA. Information that constitutes an unwarranted invasion of personal privacy under the FOIA shall not be released without the consent of the individual who is the subject of the requested record. Information in personnel and medical files is an example of records, the disclosure of which, may be an unwarranted invasion of personal privacy.

To determine if a release would result in an "unwarranted invasion of personal privacy" consideration should be given to the stated purpose of the request. To determine if a release is "clearly unwarranted," the public interest in requesting the information must be balanced against the sensitivity of the privacy interest being threatened. See figure 11-3 for points to consider when

determining whether or not to release information. Should conflict exist, the protection of personal privacy will prevail. Information should not be withheld from the individual's designed legal representative unless an exemption applies. An unwarranted invasion of the privacy of others discussed in that record may, however, constitute a basis for deleting reasonable segregable portions of the record even when providing to the subject of the record.

b. Military. Information that may be released on military personnel under the FOIA is contained in Figure 11-1. This figure may be used as a quick reference of some of the information that is releasable.

(1) Decedents. The definition of the term "individual" in the Privacy Act clearly implies that the statute only applies to living persons. The FOIA, however, authorizes withholding of certain data from the decedents' records to protect the privacy of next of kin or other living persons.

(2) Home of Record/Present Home Address/Home Telephone Number. No general rule for disclosure of an individual's home of record can be adopted because of the widely differing circumstances that are present in requests for this item of information. As the facts and needs will differ in each circumstance, a balancing test must be made on a case-by-case basis. However, home of record may usually be released if no street address is given. In most cases, an individual's geographical location; i.e., Clinton, Maryland, may be provided but not the individual's street address. The release of an individual's present home address (which includes barracks and Government-provided quarters) and/or home telephone number is normally considered a clearly unwarranted invasion of personal privacy and release is prohibited. Requests for home addresses may be forwarded to the last known address of the individual for reply at the individual's discretion. The requester will be notified of the referral. Release may be permitted without prior consent of the individual if:

(a) The individual has indicated there is no objection to release of their home address and/or telephone number.

(b) The source of the information is a public document; e.g., commercial telephone directory.

(c) The release is required by Federal statute or law; e.g., to a federally funded program to locate fathers who have defaulted on child support or collection of alimony. Prior to release, the reason

for such release shall be documented.

(d) The releasing official determines as a result of a balancing test, that circumstances of the case weigh in favor of release. When applying a balancing test, the interest of the individual in maintaining privacy from unnecessary public scrutiny must be weighed against the interest of the

public to have information about Government affairs. The reason(s) for determining release of information shall be documented. Refer to figure 11-3 for general guidance in applying the balancing test.

(3) Awards and Decorations/Citations. Releasable. The presentation of an award, decoration and/or appropriate citation is generally a public event, usually the subject of some publicity in the local facility newspaper, and in the case of most awards and decorations there is a visible token thereof worn upon the uniform.

(4) Education/Schooling/Specialty. Releasable. SECNAVINST 5211.5 provides that such information may be released. Information as to the major area of study, school, year of graduation, degree and specialty designator, are generally releasable under FOIA.

(5) Race. In Most Cases(s), Not Releasable. To release information from departmental records regarding race may constitute an unwarranted invasion of privacy. It is recognized, however, that on occasion a specific request may be made for such information in circumstances in which it is relevant; e.g., a racially oriented protest or altercation. Where the fact of an individual’s race is relevant in providing essential facts to the press, it may be released.

(6) Character of Discharge

(a) Administrative. Not Releasable. The character of discharge resulting from administrative processing is not a matter of public record. Do not release any indication of whether a discharge is honorable, general, or undesirable. The DoD has gone to great lengths to preserve the confidentiality of the character of discharge, including the removal of separation designation numbers from the DD Form 214. The release of this information to the general public has thus been view as an unwarranted invasion of personal privacy and not releasable under the Privacy Act unless the individual provides written consent.

(b) Punitive. Releasable. In the case of discharge resulting from court-martial, the proceedings and record are exempt from the restrictions of the Privacy Act because that Act incorporates the definition of "agency" found at 5 U.S.C. 551(1) which specifically excludes court-martial (see 5 U.S.C. 551(1)(F). The proceedings are public. Therefore, the approved sentence and subsequent clemency action, if any, are releasable.

(7) Duty Status. Releasable. The release of information regarding duty status is permitted to include relevant dates, as specified in appropriate departmental directives. Release of information such as the fact of unauthorized absence/desertion, hospitalization, in hands of civil authorities awaiting trial, and confinement by military authorities awaiting trial is permitted.

(8) Decisions of Personnel Records. Releasable after decision by final approving authority if the board action applies to a category of persons, as opposed to an individual. Otherwise, the records are not releasable.

(9) Photographs in the Custody of the DoD. Photographs of DoD military and civilian personnel taken for official purposes are generally releasable unless the photograph depicts matters that if disclosed to public view would constitute a clearly unwarranted invasion of personal privacy. Generally, award ceremony photographs, official selection file photographs, chain of command photographs, and similar photographs are releasable. Photographs of Marine Corps military and civilian members which contain certain personal information, such as the SSN and home address, on the reverse side shall be deleted prior to the release.

(10) Court-Martial Proceedings. JAGINST 5800.7, Manual of the Judge Advocate General (JAG), Paragraph 0142, addresses the release of information in cases involving court-martial proceedings. Essentially, this Manual lists information about a person accused or suspected of an offense which may be released. Circumstances may dictate the release of additional information or the nonrelease of the information cited in the JAG Manual. In such cases, the senior judge advocate of the command involved shall be responsible for determining whether questionable material shall be released. The final decision of a court-martial is releasable to the public.

c. Civilians. Information releasable under the FOIA on civilian employees is shown in figure 11-2. Rules applicable to civilian personnel may vary substantially from what is considered releasable on military personnel. Requests for information submitted by labor organizations citing decisions of the Federal Labor Relations Authority, Public Law 95-454, or 5 U.S.C. Section 7114 as the basis for the request, should be coordinated with the local labor relations advisor. Refer to 5 C.F.R. Sections 294 and 297 for further guidance on releasable information on civilian personnel.

4. Applicability to Deceased Persons. Data pertaining to deceased service members/employees may be released under the Privacy Act; i.e., dates of service, date and place of birth, place of burial, etc. Although the Privacy Act was not designed to protect the records of deceased individuals from disclosure, discretion should always be used when information about decedents is released. This practice will protect the privacy of next of kin and it is keeping with the spirit and intent of the Act. In unusual

circumstances, the FOIA authorities withholding of some data to protect the privacy of next of kin.

5. Providing Wage and Earning Statements (W-2 Forms) for Military Personnel to State and Local Tax Authorities. The information contained on W-2 Forms is required to be disclosed to state and local taxing authories under the FOIA. No accounting of such disclosures is required.

6. Mailing Lists. Disclosure of unclassified lists of names and duty addresses or duty telephone numbers of members assigned to units that are stationed in foreign territories, routinely deployable or sensitive can constitute a clearly unwarranted invasion of personal privacy. Lists that fall in these categories may be withheld under exemption (b)(6) of the Freedom of Information Act. Disclosure of such information poses a security threat to those service members because it reveals information as to their degree of involvement in military actions in support of national policy, the type of unit they are attached to, and their absence from their households. Release of such lists aids the targeting of service members and their families by terrorists or other persons opposed to implementation of national policy. Only an extraordinary public interest in disclosure of this information can outweigh the need and responsibility of the Marine Corps to protect service members and their families, especially those who have been subjected to harassment, threats, and physical injury. This policy applies to the following types of units:

(1) Units located outside the 50 states, District of Columbia, Commonwealth of Puerto Rico, Guam, U.S. Virgin Islands, and American Samoa.

(2) Routinely Deployable Units. Those units forming the core of the operating forces; for example, organized, equipped, and specially tasked to participate directly in strategic or tactical operations. These units normally deploy from home port or permanent station on a periodic or rotating basis to meet operational requirements or participate in scheduled exercises. This includes all Fleet Marine Forces.

(3) Units Engaged in Sensitive Operations. These are units involved in covert, clandestine, or classified missions, (to include units involved in collecting, handling, or storing classified information and materials). This also includes units involved in training or advising foreign personnel.

Exceptions to this policy must be coordinated with the CMC (ARAD) prior to responding to the requester, including request for this type of information from Members of Congress.

7. Civilian Employees Addresses. Disclosure of addresses of Marine Corps civilian employees is governed by OPM regulations.

THE PRIVACY ACT OF 1974

RELEASABLE INFORMATION ON MILITARY

Name

Grade

Date of Rank

Duty Status at Any Given Time

*Present and Past Duty Station

*Future Assignments that are Officially Established

*Office or Duty Telephone Numbers

Source of Commission

Attendance at Professional and Military Schools (Major Area of Study, School, Year of Graduation and Degree)

Promotional Sequence Number

Decorations and Medals

NOTE: Items listed above are not all inclusive of information that may be releasable.

*See paragraph 11000.6 for additional guidance on release of official or duty station addresses and telephone numbers.

Figure 11-1.--Releasable Information on Military.

THE PRIVACY ACT OF 1974

RELEASABLE INFORMATION ON CIVILIANS

Name

Present and Past Position Titles

Present and Past Grades

Present and Past Salaries

Gross Salary

Present and past duty stations (which includes room numbers, shop designation, or other identifying information regarding buildings or places of employment)

Disclosure of other personal information pertaining to civilian employees shall be made in accordance with the Federal Personnel Manual, Chapter 294, subchapter 7.

Figure 11-2.--Releasable Information on Civilians.

THE PRIVACY ACT OF 1974

POINTS TO CONSIDER WHEN APPLYING THE BALANCING TEST FOR DETERMINATION OF RELEASE OF INFORMATION

NOTE: The following points are not inclusive, but may be used as a basic tool for evaluation.

1. Do individuals normally have an expectation of privacy in the type information being considered for disclosure?

2. Is the information readily available elsewhere from public sources?

3. What is the public interest to be served by the release?

4. What relationship exists between the proposed recipient and the public interest to be served by release, if any?

5. Will the individual to whom the record pertains gain any benefit from the release? If so, is this a significant benefit or only a marginal one?

6. What are the possibilities of other invasions of personal privacy which might result from further release of the information by the intended recipient?

7. Is the individual to whom the information pertains particularly newsworthy or a public figure?

8. How sensitive is the information to be released to the individual or family?

9. How old is the information? (For example, 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.)

10. Has the information been made public as a result of a trial or public hearing?

11. How much knowledge does the requester have of the information requested?

Figure 11-3.--Points to Consider When Applying Balancing Test.

CHAPTER 12

INSTRUCTIONS FOR ANNUAL PRIVACY ACT REPORT AND OTHER INFORMATION REQUIREMENTS

CHAPTER 12

INSTRUCTIONS FOR ANNUAL PRIVACY ACT REPORT AND OTHER INFORMATION REQUIREMENTS

12000. GENERAL. An annual report will be submitted to the Congress on records systems maintained by the Marine Corps. The annual report contained in this Manual is based on the OMB guidance and supersedes the previous report. The report control symbol assigned this report is DD-5211-01.

1. Reporting Responsibilities

a. Marine Corps commanders will be responsible for preparing and submitting a consolidated report for their headquarters and subordinate activities, to the CMC (ARAD) by 1 February of each year.

b. The CMC (ARAD) is responsible for preparing the consolidated Marine Corps report, for submission to the Chief of Naval Operations by 28 February of each year and further transmittal of the OMB.

c. Marine Corps units that are afloat and operational aviation squadrons who have not received or responded to a Privacy Act request during the reporting period are exempt from this reporting requirement.

2. Reporting Requirements

a. Prepare and submit to the CMC (ARAD) the consolidated annual report using NAVMC 11326 (2-95) (EF) (figure 12-1). Commanders and headquarters staff agencies shall establish procedures to ensure that responsible personnel are alerted to accumulate and maintain throughout the calendar year, all the appropriate information, data, facts and statistics necessary for input to the report.

b. NAVMC 11326 is accessible in the Marine Corps Electronic Forms System (MCEFS) as well as the normal supply channels. MCEFS provides the capability to complete, save, transmit and print forms/forms data. For additional information on MCEFS, contact your G-1/S-1 or forms management area.

3. Disposition Guidance. Copies of annual reports maintained by Marine Corps commanders may be destroyed 2 years after submission to CMC (ARAD).

12001. LITIGATION STATUS SHEET. When a complaint citing the Privacy Act is filed in a U.S. District Court against the Marine Corps, or any Marine Corps employee, the responsible system manager shall notify promptly the CMC (ARAD). A sample litigation status sheets requires, at‘ minimum, the information listed in figure 12-2. Revised litigation status sheets are required at each stage of the litigation. Copies of the formal opinion or judgment will be provided to the CMC (ARAD).

THE PRIVACY ACT OF 1974
PRIVACY ACT - ANNUAL REPORT

1. POINT OF CONTACT: Provide the name, title, and telephone number of the individual who is responsible for preparing this report.

NAME:	TITLE:	TELEPHONE NUMBER:

2. EXERCISE OF INDIVIDUALS RIGHTS: This report requests the number of times individuals requested records from systems of records concerning themselves. Count only those instances where the individual has cited the Privacy Act or some implementing instructions to gain access to or requested amendment of their records.

DESCRIPTION OF ACTIONS TAKEN	NUMBER RECEIVED
a. Total number of requests for access:	
b. Number of requests wholly or partially granted:	
c. Number of requests totally denied:	
d. Number of requests for which no record was found:	
e. Number of requests to amend records in system:	
f. Number of amendment requests wholly or partially granted:	
g. Number of amendment requests totally denied:	

h. If your agency denied an individual access to their records on any basis other than a Privacy Act exemption ((j) or (k)), describe below and provide the legal justification for the denial (use continuation sheet if needed):

3. Recommendations for Administration/Legislative Changes: Identify problems, indicate their effect on agency activities, and submit recommendations for the change.

REPORT CONTROL SYMBOL DD-[illegible]

NAVMC 11326 (2-95) (EF)
SN: 0109-LF-067-0600

Figure 12-1.--Content for Annual Report.

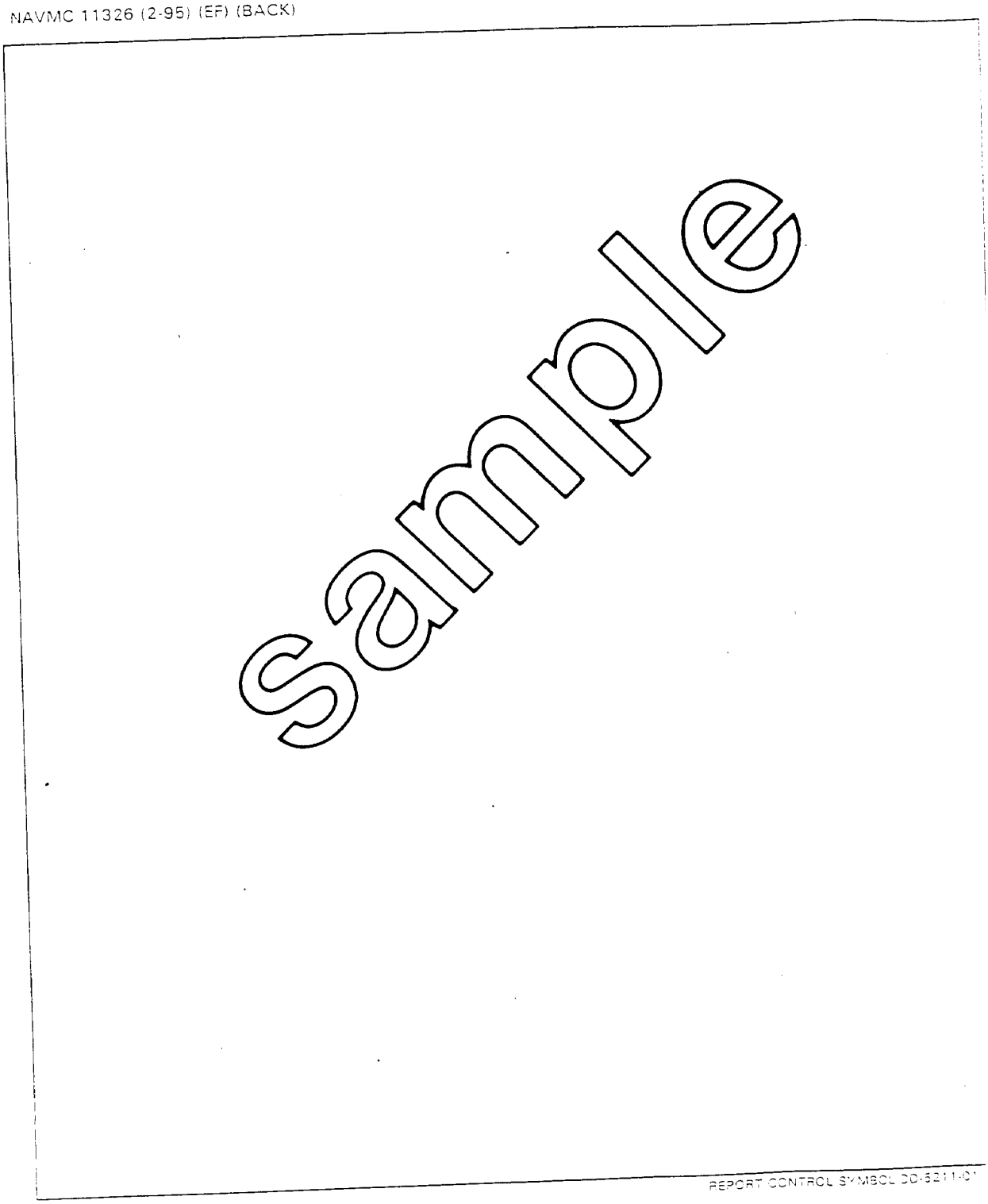


Figure 12-1.--Content for Annual Report--Continued.

LITIGATION STATUS SHEET

1. Case Name and Number:

2. Plaintiff(s):

3. Defendent(s):

4. Basis for Court Actions:

5. Initial Litigations:

   a. Date Complaint or Charges Filed:

   b. Court:

   c. Court Action:

6. Appeal (if any):

   a. Date Appeal Filed:

   b. Courts:

   c. Case Number:

   d. Court Ruling:

7. Remarks:

Figure 12-2.--Litigation Status Sheet.

CHAPTER 13

TRAINING

CHAPTER 13

TRAINING

13000. TRAINING REQUIREMENTS. The Privacy Act requires the Marine Corps to conduct training for all personnel involved in the design, development, operation, or maintenance of any systems of records. All such personnel will be instructed in the principal provisions of the Act.

1. Objectives. To satisfy this requirement, the following objectives are established:

a. Orientation. To provide orientation to the design, development, operation, or maintenance of any systems of records in the principal provisions of the Privacy Act, include as a minimum the following:

(1) Background and Scope.

(2) Explanation of Terms.

(3) Responsibilities.

(4) Access, Amendment, and Notification Procedures.

(5) Collection of Information from Individual.

(6) Disclosure Procedures.

(7) Safeguarding Personal Information.

(8) Systems of Records.

(9) Exemptions.

(10) Rules of Release of Information.

b. Working Knowledge. Provide a specific working knowledge of the principal provisions of the Privacy Act to all Marine and civilian personnel whose normal duties include maintenance of personal information which is part of a record or system of records.

2. Responsibility. Commanders will be responsible for the orientation and training of the principal provisions of the Privacy Act to all Marines and civilian personnel whose normal duties

include the maintenance of personal information. The Commandant of the

Marine Corps (ARAD) will be responsible for providing training or access to training for all Marines and civilian employees of the Headquarters staff agencies. Figure 13-1 provides a suggested vehicle and may be developed with slides for training.

THE PRIVACY ACT OF 1974

PRIVACY ACT SCRIPT

Slide 1 - INTRODUCTION

The Privacy Act requires each Federal agency to train all personnel involved in the design, development, operation, and maintenance of records system subject to the Act. Since the law is very technical and subject to interp-retations, this training session is designed to provide a broad overview and should serve as an orientation for new personnel.

Slide 2 - BACKGROUND

To better understand why the Privacy Act was put into law, it may be helpful to provide you with some background.

In recent years, both in and out of Government, there has been a vast increase in the amount of data collected on individuals.

In part, the rapid growth of computer technology magnified the problem and increased the potential to violate the individual’s privacy.

Although it appeared that we had sufficient safeguards to protect the individual, there was a flagrant misuse of the data, which in some cases was used to harm an individual. (Give examples of situations which have appeared in the news media reports, etc.)

As a result, Congress saw the need to reassert the constitutional rights of an individual.

Hence, the enactment of the Privacy Act (P.L. 93-579).

Slide 3 - FEATURES

I’m sure you have heard the words "Privacy Act," but can you really define what the Act is all about and more importantly, do you really understand how it protects you? There are two primary features of the Privacy Act:

(1) It provides safeguards against any invasion of personal privacy.

(2) It enables individuals to gain access to records pertaining to themselves.

Figure 13-1.--Training Script.

THE PRIVACY ACT OF 1974

Slide 4 - APPLICABILITY

The Privacy Act applies to:

- Only Federal agencies within the Executive Branch of Government. This includes the military departments.

- Any commercial contractors hired to accomplish a Government mission and who maintains or access files containing personal information.

- Systems of records where information is retrieved by a personal identifier, such as the name, social security number, fingerprint, photograph, etc.

As you can see, the Act encompasses almost all the files that you are familiar with.

Slide 5 - HE PRIVACY ACT VERSUS FREEDOM OF INFORMATION ACT

It may be beneficial at this point to talk briefly about the Freedom of Information Act and the relationship between the Privacy Act and the Freedom of Information Act.

In case you are unclear about the Freedom of Information Act, it can be explained as follows:

- The Freedom of Information Act was designed to enable the public to obtain information about an agency.

- The Privacy Act enables individuals to request information about themselves.

Many believe that these acts conflict, but this is not so. In briefest terms, personal information is usually considered private--information about an agency and the way it conducts its business is usually considered public.

Slide 6 - RELEASABLE INFORMATION (MILITARY)

There are certain items of information which are releasable to the public without invading an individual’s privacy. (Refer to figure 11-1 of this Manual for items that are releasable under the Freedom of Information Act on military personnel.) This means that prior consent by the individual for release of information is not necessary.

Although some of the information may appear to be personal and thus protected by the Privacy Act, it has been determined to be of public record and, therefore, not an invasion of one’s privacy.

Figure 13-1.--Training Script--Continued.

13-6

THE PRIVACY ACT OF 1974

Slide 7 - RELEASABLE INFORMATION (CIVILIANS)

Certain items of information are releasable on civilian personnel without consent of the individual concerned. You may release the items of information listed (refer to Figure 11-2), but for further guidance on releasable information on civilians refer to the Federal Personnel Manual, chapter 294, subchapter 7 or contact the civilian personnel office.

Slide 8 - RIGHTS AND RESPONSIBILITIES

Now that you know why this law was enacted, let's talk about your rights and responsibilities under the Act.

- The Act requires that you be entitled to know just what records are being maintained on you and to expect that no unauthorized information will be used to make unfair determinations.

- Records gathered for one purpose cannot be used for another without your consent. For example: Home addressees collected for inclusion in an emergency recall roster could not then be used for a social roster unless both have been previously identified.

- You can review your records at any time, in a comprehensible form and request a copy be made of any portion of that file. You may be charged duplication fees but no search fees. Under the Freedom of Information Act, however, you could be charged for any retrieval cost and/or search fees associated with obtaining the information to satisfy your request.

Slide 9 - NO SECRET FILES

No secret files are allowed to be maintained on an individual. I'm not talking about classified files, I'm talking about the "mere existence" of a record which prior to the enactment of the law, may have been hidden. Just stop and think for a moment, do you know of any files which the pubic does not know exist?

There are some records which are exempt from disclosure to individuals, however, their existence must at least be identified. There is a distinct difference between a record existing and an agency being required to disclose it contents.

Slide 10 - FEDERAL REGISTER

In order to properly and legally maintain files, a requirement exists to publish a listing in the Federal Register of all systems of records which the Marine Corps maintains and are retrieved by a personal identifier. The notices include such categories as:

Figure 13-1.--Training Script--Continued.

THE PRIVACY ACT OF 1974

- A description of files.

- Instructions on how to request access.

- Who to contact for assistance.

For those who are unfamiliar with the Federal Register, it is a daily publication of regulations and legal notices issued by Federal agencies. They can be found in any Marine Corps legal office and also in any public library. (If the Federal Register is not available, refer to the current publication in Marine Corps Order 5211 series showing system notices under the Privacy Act.)

Slide 11 - ORGANIZATIONAL RESPONSIBILITIES

The Marine Corps can only maintain information that is required by law/ Executive Order or is relevant and necessary to carry out its mission. No longer can we collect information because it is nice to have or perhaps it is anticipated that the information will be needed in the future. The primary objective of the Act was to report information as accurately as is feasible. To accomplish this objective, collect information directly from the individual, not from friends, third parties, or acquaintances.

There are several precise requirements which must be satisfied when collecting information. You must inform the individual:

- Under what authority (statute/Executive Order).

- Purposes. For example, the information is required to process an ID card.

- Routine uses; i.e., what use will be made of the information; will it be used for promotion, or assignment, or training, etc.?

- Whether the information solicited is mandatory or voluntary.

- The effect of not providing the requested information. Please note, however, that the effects should never be viewed as a threat to the individual.

The Privacy Act statement should be brief and easily understood. It can be part of the form, attached as a separate sheet, or conspicuously posted in the working area in which the information is collected. Everyone has been requested to sign at least one of these statements. The Marine Corps recognized the administrative burden associated with the development of the statement and

Figure 13-1.--Training Script--Continued.

designed a blanket statement for the collection of information concerning personnel and pay matters. Once each individual signs the blanket statement, it is permanently placed in the individual's record and this authorizes the Marine Corps to collect/solicit any type of information from the individual associated with their personnel record and/or pay.

Another responsibility of the Marine Corps is to publish notice in the Federal Register of all systems of records from which information is retrieved by a personal identifier. When the Act was first implemented, all Federal agencies were required to publish notice of their systems. At present, the Marine Corps maintains approximately 100 systems. For those who are unfamiliar with the Federal Register, it provides a means by which the public can learn about the activities of the Government agencies. Anyone who wants to know whether an agency is keeping records which might pertain to them can find out by checking the Federal Register.

Another requirement of the Privacy Act states that we must establish more positive safeguards to protect to protect the security and confidentiality of personal data. This applies to both paper records such as the OQR/SRB as well as automated records.

Each office maintaining or accessing personal information must now establish administrative, technical and physical safeguards to ensure the confidentiality of records and to protect against any threats which could result in substantial harm, embarrassment or unfairness to the individual.

- We must restrict access to those who require the records in the performance of their official duties (a need to know) or to the individual who is the subject of the record or an authorized representative.

- All personal information shall be treated as "For Official Use Only."

- All information must be stored in locked metal filing cabinets or behind locked rooms when you secure for the day.

- All information which is no longer needed shall be torn or destroyed to preclude recognition or reconstruction. There is an exception to this rule. We recognize that it would be more difficult to identify information about individuals in bulk quantities, such as punch cards, computer printouts, and other bulky products. These may be destroyed via the normal trash cycles for scrap or recycling.

The case with which our personnel use remote terminals to query the Marine Corps Total Force System, for example, necessitates close control also.

Figure 13-1.--Training Script--Continued.

THE PRIVACY ACT OF 1974

- We should limit access to personal information via our on-line terminals only to authorized individuals having a need to know. Lists should always be posted as to who is allowed to use the terminals.

- Establish positive identification via passwords, access lists, and controlled areas.

- Supervisors must enforce periodic checks of computer-operated output either by means of internal audit procedures or data base access accounting reports.

- Always be provided positive identification or authorization prior to releasing information to any individual.

- Files not subject to the Privacy Act but created from files known to contain personal information, must be examined to ensure that they cannot be used to regenerate any personal information and used for other purposes.

- Label any output and storage media containing personal information to warn individuals of the presence of personal data and the need for proper handling. (For example: Restricted Area--Authorized Personnel Only.)

All areas or facilities that process or contain personal information should be designated as controlled areas and identified accordingly.

Always remember that passwords must be periodically changed. Passwords should never be assigned to individuals based on characteristics such as initials, birth date, or telephone number. All too often we are careless on how we store, safeguard, or dispose of files. There is a constant need for security and safeguarding personal information.

The Privacy Act requires that the Marine Corps conduct training/orientation for all active duty and Reserve personnel and each civilian employee in the basic provisions of the Act. If the individual’s normal duties include the maintenance of personal information which is part of a system of records, the law requires that those individuals be knowledgeable in the principal provisions of the Act, and annually briefed on any major changes/amendments or new guidance issued to continue the effective administration of the Privacy Act.

The submission of the annual report on privacy matters appears to create the most confusion from the field activities. The following highlights some of the major problem areas field activities are experiencing when preparing the annual report.

- The content/format may change each year. This is a fact of life and until higher authorities develop a standard format for submission of the report, commands must continue to maintain the statistics requested.

- Since Congress is concerned about the impact of this legislation on the public, each activity will be queried annually concerning the number of requests received for access/amendment to its records. Recommend that each activity continue to maintain an accurate accounting of those requests in a method that is easily retrievable for future submissions even though this format could be revised.

Slide 12 - DISCLOSURE

Questions most frequently asked relate to the disclosure provision.

The general rule for disclosure is: Information cannot be disclosed without the consent of the individual concerned. However, there are exceptions to the rule. Information may be disclosed without the individual's consent to:

- Department of Defense personnel with a need to know. For example, a pay clerk may have access to an individual's personnel record in order to resolve a particular pay discrepancy.

- Requests which the information is required to be released under the Freedom of Information Act.

- A routine user, if that agency has been previously identified as such in a system notice.

- The Bureau of Census when conducting a census.

- Requests for statistical research if the information does not identify individual's by name or other personal identifier. For example, if information is requested on how many high school graduates versus non-high school graduates have disciplinary problems, that statistic would be releasable.

- The National Archives for historical purposes.

- An agency or individual in an emergency or compelling situation affecting the health and/or safety of an individual.

- A law enforcement agency if the request is in writing and on official letterhead.

Figure 13-1.--Training Script--Continued.

- A congressional committee in the performance of its duties to the extent of matters within its jurisdiction or to a Congressman, made at the request of the Congressman's constituent.

- General Accounting Office in the performance of its duties.

- And to the courts.

It is relatively easy to obtain information about yourself. If you still believe, however, that this whole law has created an administrative burden and was not necessary, always remember that the Act was designed to protect your privacy and to restrict others from obtaining information about you.

Slide 13 - DISCLOSURE WITHOUT CONSENT

No disclosure without consent. This is a key point!

Slide 14 - DISCLOSURE ACCOUNTING

Another important provision of the Act cites that each individual has the right at any time to request an accurate accounting of information disclosed about them to an agency outside of the Department of Defense. In order for the Marine Corps to fulfill this requirement, it must keep an accurate accounting of the day, nature, purpose and person/agency that the information was disclosed.

The Marine Corps must retain these accounting records for 5 years or the life of the record, whichever is longer.

These records must be made available at any time to the requesting individual. This will permit you to know precisely how and what information about you is used.

Slide 15-ACTION/CORRECTION

Each employee with the Marine Corps has the right to be notified of the existence of records that pertain to the individual, to have access to those records, to copy them, and to have them amended if they are not accurate, relevant, timely, and complete.

The second part of this slide addresses the Marine Corps responsibilities.

- Upon receipt of the request for notification, access or amendment to a particular system of records, the Marine Corps has 10 days to acknowledge the request.

Figure 13-1.--Training Script--Continued.

- When a request to amend a record is received, the Marine Corps will review the request and decide whether the request should be granted or denied. If the reviewing official agrees with the initial request to amend the record, the record will be amended accordingly. If the reviewing official denies the initial request to amend the record, the requesting individual will then be advised of the right to appeal to the Secretary of the Navy for correction of the record.

- Upon receipt of the request for administrative review by the Secretary of the Navy, the review shall be acted on within 30 days and the individual informed of the final determination. If it is determined that the request should be granted, in whole or in part, the system manager shall be directed to take appropriate action to amend the record. If it is determined that the request should be denied, the requesting individual shall be informed of the reasons thereof and the right to seek judicial relief in the Federal courts.

Slide 16 - EXEMPTED RECORDS

Under certain circumstances, all or portions of a file may be withheld from you but only to the extent that the release of the data may:

- damage national security;

- impede a law enforcement activity; or

- reveal the identity of a confidential source.

There are certain categories of information which are subject to either a general or specific exemption.

The general exemption category applies to information maintained by either the CIA or compiled for criminal law enforcement purposes. The Marine Corps has claimed this exemption for the Base Security Incident Reporting System.

The specific exemption category relates to such files as:

- those classified for national defense;

- investigations compiled for law enforcement purposes or determining suitability for employment;

- for statistical research;

Figure 13-1.--Training Script--Continued.

- providing protective services for the President; and

- for test/examination material such as the recruiting test or the Civil Service test administered for employment.

The Marine Corps has claimed this exemption for the Personnel Security Eligibility and Access Information System.

Slide 17 - NONCOMPLIANCE

There are penalties if you fail to comply with the provision of the Privacy Act. You could be penalized for:

- Maintaining secret data or file.

- Willfully disclosing information to unauthorized personnel.

- Disclosing information under false pretenses.

Slide 18 - PENALTIES

What are the penalties?

- The agency, in this case, the Marine Corps, would be sued.

- The individual involved would be charged with a misdemeanor and fined up to $5,000.

CONCLUSION

Now that you have all been briefed on the basis provisions of the Privacy Act, MCO P5211.2B is the document which fully outlines the rules and procedures that must be followed in your daily duties. If any questions arise, be sure to contact the local Privacy Act Coordinator or the Privacy Act Coordinator for the Marine Corps (ARAD).

Figure 13-1.--Training Script--Continued.