DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

SECNAVINST 5211.5E
DNS-36
28 Dec 2005

SECNAV INSTRUCTION 5211.5E

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY (DON) PRIVACY PROGRAM

Ref: (a) 5 U.S.C. 552a
(b) DOD Directive 5400.11 of 26 Nov 04
(c) DOD 5400.11-R of 31 Aug 83
(d) DOD Directive 5100.3 of 15 Nov 99
(e) 5 U.S.C. 552
(f) SECNAVINST 5720.42F
(g) E-Government Act of 2002 (Public Law 107-347)
(h) DOD Memo of 28 Oct 05, subject: "DOD PIA Guidance"
(i) SECNAVINST 5720.47B
(j) SECNAVINST 5210.8D
(k) DOD Directive 6025.18 of 19 Dec 02
(l) DOD 6025.18-R of 24 Jan 03

1. Purpose. To implement references (a), (b) and (c); to ensure that all DON military members and civilian/contractor employees are made fully aware of their rights and responsibilities under the provisions of the Privacy Act (PA); to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy stemming from the DON's collection, maintenance, use, and disclosure of Protected Personal Information (PPI); and to require privacy management practices and procedures be employed to evaluate privacy risks in publicly accessible DON web sites and unclassified non-national security information systems.

a. Scope. Governs the collection, safeguarding, maintenance, use, access, amendment, and dissemination of PPI kept by DON in PA systems of records.

b. Guidance. Provides guidance on how to respond to individuals who seek access to information in a PA system of records that is retrieved by their name and/or personal identifier.

c. Verify Identity. Establishes ways to verify the identity of individuals who request their records before the records are made available to them.

d. Online Resources. Directs the public to the Navy's PA Online web site at http://www.privacy.navy.mil that defines the DON's PA Program, lists all Navy, Marine Corps, and Government-wide systems of records and provides guidance on how to gain access to those records.

e. Rules of Conduct. Governs the PA rules of conduct for personnel, who will be subject to either civil or criminal penalties for noncompliance with reference (a).

f. Privacy Impact Assessment (PIA) Requirements. Establishes requirements for conducting, reviewing, approving, and publishing PIAs.

This instruction is published at 32 C.F.R. Part 701, subparts F and G. It is a complete revision and should be read in its entirety.

2. Cancellation. SECNAVINST 5211.5D and Annual PA Report.

3. Summary of Changes

a. Eliminated enclosures by making them available on the DON's PA web site at http://www.privacy.navy.mil allowing more frequent updating or by incorporating them in the text of this instruction.

b. Defined and expanded roles of officials with regard to implementation and compliance with PA.

c. Added guidance on PPI.

d. Streamlined procedures for creating, deleting, amending, and altering PA systems of records notices.

e. Removed detailed guidance on computer matching, since all actions are reviewed at the CNO (DNS-36) level and approved by the membership of the Defense Data Integrity Board.

f. Established a DON PA Oversight Working Group to coordinate and review departmental PA practices.

g. Added guidance on conducting PIAs.

4. Privacy Program Terms and Definitions

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

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

c. Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review), to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

d. Federal Personnel. Officers and employees of the U.S. Government, members of the uniformed services (including members of the reserve), individuals or survivors thereof, entitled to receive immediate or deferred retirement benefits under any retirement program of the U.S. Government (including survivor benefits).

e. Individual. A living citizen of the U.S. or an alien lawfully admitted to the U.S. for permanent residence. The custodial parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

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

g. Information in Identifiable Form (IIF). Information in an IT system or online collection that directly identifies an individual (e.g., name, address, social security number or other identifying code, telephone number, email address, etc) or by an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification that may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

h. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information.

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

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

k. Minor. Under this instruction, a minor is an individual under 18 years of age, who is not a member of the U.S. Navy or Marine Corps, or married.

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

m. Personal Information. Information about an individual that identifies, relates, or is unique to, or describes him or her (e.g., SSN, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.).

n. Privacy Act (PA) Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

o. Privacy Impact Assessment (PIA). An ongoing assessment to evaluate adequate practices in balancing privacy concerns with the security needs of an organization. The process is designed to guide owners and developers of information systems in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, identifying and resolving the privacy risks, and approval by a designated privacy representative.

p. Protected Personal Information (PPI). Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records.

q. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc), about an individual that is maintained by a DON activity including, but not limited to, the individual’s

education, financial transactions, and medical, criminal, or employment history, and that contains the individual's name or other identifying particulars assigned to the individual, such as a finger or voice print or a photograph.

r. Review Authority. An official charged with the responsibility to rule on administrative appeals of initial denials of requests for notification, access, or amendment of records. SECNAV has delegated review authority to the Assistant Secretary of the Navy (Manpower & Reserve Affairs) (ASN (M&RA)), General Counsel of the DON (GC), and the Judge Advocate General of the Navy (JAG). Additionally, the Office of Personnel Management (OPM) is the review authority for civilian official personnel folders or records contained in any other OPM record.

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

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

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

v. System of Records. A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all PA systems of records must be published in the Federal Register and are also available for viewing or downloading from the Navy's Privacy Act Online web site at http://www.privacy.navy.mil.

w. Web Site. A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the "home page" and the linked subordinate information.

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

5. Online Resources

a. Navy PA Online Web Site (http://www.privacy.navy.mil). This web site supplements this instruction. It provides a detailed understanding of the DON's PA Program. It contains information on Navy and Marine Corps systems of records notices; government-wide systems of records notices that can be used by DON personnel; and identifies Navy and Marine Corps exempt systems of records notices. It includes: PA policy documents; sample training materials; Department of Defense (DOD) "Blanket Routine Uses;" a checklist for conducting staff assistance visits; a copy of PA statute; guidance on how to establish, delete, alter, or amend PA systems of records notices; and provides updates on the DON's PA Program.

b. DON Chief Information Officer (DON CIO) Web Site (http://www.doncio.navy.mil). This web site provides detailed guidance on PIAs.

c. DOD's PA Web Site (http://www.defenselink.mil/privacy). This web site is an excellent resource that contains a listing of all DOD and its components' PA systems of records notices, DOD PA directive and regulation, OMB Circulars, Defense Privacy Decision Memoranda, etc.

d. DON Freedom of Information Act (FOIA) Web Site (http://www.foia.navy.mil). This web site discusses the interface between PA and FOIA and provides detailed guidance on the DON's FOIA Program.

6. Applicability

a. DON Activities. Applies to all DON activities that collect, maintain, or disseminate PPI. Applies to DON activities and to contractors, vendors, and other entities that develop, procure, or use Information Technology (IT) systems under contract to DOD/DON, to collect, maintain, or disseminate Information in Identifiable Form (IIF) from or about members of the public.

b. Combatant Commands. Applies to the U.S. Joint Forces Command (USJFCOM) and U.S. Pacific Command (USPACOM), except for U.S. Forces Korea as prescribed by reference (d).

c. U.S. Citizens and Legally Admitted Aliens. Applies to living citizens of the U.S. or aliens lawfully admitted for permanent legal residence. Requests for access to information in a PA system of records made by individuals who are not U.S. citizens or permanent residents will be processed under the provisions of the FOIA.

d. Federal Contractors. Applies to Federal contractors by contract or other legally binding action, whenever a DON contract provides for the operation, maintenance, or use of records contained in a PA system of records to accomplish a DON function.

(1) When a DON activity contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record system affected are considered to be maintained by the DON activity and are subject to this instruction

(2) The contractor and its employees are considered employees of the DON activity for purposes of the sanction provisions of the PA during the performance of the contract.

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

(4) Consistent with the FAR regulations, contracts for the operation of a system of records shall identify specifically the record system and the work to be performed, and shall include in the solicitation and resulting contract the terms as prescribed by the FAR [see http://www.privacy.navy.mil (Admin Tools)].

(5) DON activities must furnish PA Privacy Program guidance to their personnel who solicit and award of administer government contracts; inform prospective contractors of their responsibilities regarding the DON PA Program; and establish an internal system of contractor performance review to ensure compliance with the DON Privacy Program.

(6) This instruction DOES NOT apply to records of a contractor that are:

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

(b) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to a DON activity;

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

(d) Maintained by a consumer reporting agency to which records have been disclosed under 31 U.S.C. 3711;

(7) DON activities shall establish contract surveillance programs to ensure contractors comply with the procedures established by the DAR Council.

(8) Disclosing records to a contractor for use in performing a contract let by a DON activity is considered a disclosure within DON (i.e., based on an official need to know). The contractor is considered the agent of DON when receiving and maintaining the records for that activity.

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

7. Responsibility and Authority

a. Delegation. The Chief of Naval Operations (CNO) for administering and supervising the execution of references (a), (b), and (c). The Director, Navy Staff (DNS) will administer this program through the Head, DON PA/FOIA Policy Branch (DNS-36) who will serve as the Principal PA Program Manager for the DON.

b. CNO (DNS-36)

(1) Develops and implements DON policy on the provisions of the PA; serves as principal advisor on all DON PA matters; oversees the administration of the DON's PA program; reviews and resolves PA complaints; maintains the DON's PA Online web site; develops a Navy-wide PA training program and serves as training oversight manager; establishes, maintains, deletes, and approves Navy and joint Navy/Marine Corps PA systems of records notices; compiles reports that address the DON's PA Program to DOD and/or the Office of Management and Budget (OMB); conducts PA reviews as defined in OMB Circular A-130; publishes exempt systems of records in the Code of Federal Regulations; and conducts staff assistance visits/program evaluations within DON to review compliance with reference (a) and this instruction.

(2) Serves as PA Coordinator for Office of the Secretary of the Navy (SECNAV), Office of the CNO (OPNAV) and the Naval Historical Center (NHC).

(3) Represents SECNAV on the Defense Privacy Board (DPO). Per reference (b), the Board has oversight responsibility for implementation of the DOD Privacy Program.

(4) Represents SECNAV on the Defense Data Integrity Board. Per reference (b), the Board has oversight responsibility for reviewing and approving all computer matching agreements between the DOD and other Federal, State, or local government agencies, as well as memoranda of understanding when the match is internal to DOD, to ensure that appropriate procedural and due process requirements have been established before engaging in computer matching activities.

(5) Provides input to the DPO on OMB's Federal Information Security Management Act (FISMA) Report.

(6) Coordinates on all PIAs prior to the PIA being submitted to DON CIO for review and final approval. Makes a determination as to whether the new IT system constitutes a PA system of records. If it does, determines whether an existing system covers the collection or whether a new systems notice will have to be written and approved. As necessary, assists the DON activity in creating and getting a new PA system of records notice approved.

(7) Oversees the administration of OPNAV's PA program.

(8) Chairs the DON PA Oversight Working Group.

c. Commandant of the Marine Corps (CMC)

(1) Administers and supervises the execution of this instruction within the Marine Corps and maintains and approves Marine Corps PA systems of records notices. The Commandant has designated CMC (ARSF) as the PA manager for the U.S. Marine Corps.

(2) Oversees the administration of the Marine Corps' PA program; reviews and resolves PA complaints; develops a Marine Corps privacy education, training and awareness program; reviews and validates PIAs for Marine Corps information systems and submits the validation to CNO (DNS-36); establishes, maintains, deletes, and approves Marine Corps PA systems of records notices; and, conducts staff assistance visits/program evaluations within the Marine Corps to review compliance with reference (a) and this instruction.

(3) Serves as the PA Coordinator for all Headquarters, U.S. Marine Corps components, except for Marine Corps Systems Command and the Marine Corps Combat Development Command.

(4) Provides input to CNO (DNS-36) for inclusion in the Federal Information Security Management Act (FISMA) Report.

(5) Serves on the DON PA Oversight Working Group.

(6) Coordinates on all PIAs prior to the PIA being submitted to DON CIO for review and final approval, making a determination as to whether the new IT system constitutes a PA system of records. If it does, determines whether an existing system covers the collection or whether a new systems notice will have to be written and approved. As necessary, assists the DON activity in creating and getting a new PA system of records notice approved.

d. DON CIO

(1) Integrates protection of PPI into the overall DON major information system life cycle management process as defined in reference (g).

(2) Provides guidance for effective assessment and utilization of privacy-related technologies.

(3) Provides guidance to DON officials on the conduct of PIAs (see their web site at http://www.doncio.navy.mil) and oversees DON PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of IIF in that system, and the risk of harm for unauthorized release of that information. Also, DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(4) Reviews and approves all PIAs for the DON and submits the approved PIAs to DOD and OMB according to Federal and DOD guidance.

(5) Serves as the focal point in establishing and validating DON information systems privacy requirements and coordinating issues with other DOD Military Departments and Federal Agencies.

(6) Develops and coordinates privacy policy, procedures, education, training, and awareness practices regarding DON information systems.

(7) Compiles and prepares responses to either DOD or OMB regarding PIA issues.

(8) Develops and coordinates DON web privacy policy, education, training and an awareness program in accordance with DON web privacy requirements including annual web site privacy posting training with CNO (DNS-36).

(9) Provides guidance toward effective research and development of privacy-related technologies.

(10) Serves as the focal point in establishing and validating DON web privacy requirements and coordinating issues with DOD, other Military Departments, and other Federal agencies.

(11) Provides guidance on the use of encryption software to protect privacy sensitive information.

(12) Implements DON IT privacy requirements and coordinates IT information system requirements that cross service boundaries with the Joint Staff.

(13) Provides recommended changes to CNO (DNS-36) on policy guidance set forth in this instruction regarding IT

privacy policy and procedures that includes requirements/ guidance for conducting PIAs.

(14) Provides input to CNO (DNS-36) for inclusion in the FISMA Report.

(15) Serves on the DON PA Oversight Working Group.

e. The Chief of Information (CHINFO) and U.S. Marine Corps Director of Public Affairs (DIRPA). CHINFO and DIRPA, in accordance with DON CIO guidance on Department-wide Information Management (IM) and IT matters, are responsible for developing and administering Navy and Marine Corps web site privacy policies and procedures respectively per reference (i). Additionally, CHINFO and DIRPA:

(1) Maintains master World Wide Web page to issue new service-specific Web privacy guidance. CHINFO will maintain a master WWW page to issue DON guidance and DIRPA will link to that page. All significant changes to this Web site and/or its location will be issued via Naval (ALNAV) message.

(2) Maintains overall cognizance for DON and U.S. Marine Corps web sites and web site content-related questions as they pertain to web site privacy requirements.

(3) Ensures that public-facing web sites have machine-readable privacy policies (i.e., web privacy policies are P3P-enabled or automatically readable using some other tool).

(4) Provides input to CNO (DNS-36) for inclusion in the FISMA Report.

(5) Serves on the DON PA Oversight Working Group.

f. DON PA Oversight Working Group: The DON PA Oversight Working Group is charged with reviewing and coordinating compliance with DON PA program initiatives. CNO (DNS-36) will chair this working group, hosting meetings as deemed appropriate to discuss best PA practices, PA issues, FISMA reporting and other reporting requirements, PA training initiatives, etc. At a minimum, membership shall consist of CNO (DNS-36), DON CIO, CMC (ARSF), CMC (C4I-IA), OJAG (Code 13), OGC (PA/FOIA), CMC (JAR), CHINFO, and CMC (PA).

g. DON Activities. Each DON activity is responsible for implementing and administering a PA program under this instruction.

h. Navy Echelon 2 and 3 Commands and Marine Corps Major Subordinate Commands. Each Navy Echelon 2 and 3 Command and Marine Corps Major Subordinate Command will designate a PA Coordinator to:

(1) Serve as principal point of contact on PA matters.

(2) Advise CNO (DNS-36) promptly of the need to establish a new Navy PA system of records; amend or alter an existing Navy system of records; or, delete a Navy system of records that is no longer needed.

(3) Advise CMC (ARSF) promptly of the need to establish a new Marine Corps PA system of records; amend or alter an existing Marine Corps system of records; or, delete a Marine Corps system of records that is no longer needed.

(4) Ensure no official files are maintained on individuals that are retrieved by name or other personal identifier without first ensuring that a system of records notice exists that permits such collection.

(5) Ensure that PA systems of records managers are properly trained on their responsibilities for protecting PPI being collected and maintained under the DON PA Program.

(6) Provide overview training to activity/command personnel on the provisions of reference (a) and this instruction.

(7) Issue an implementing instruction which designates the activity’s PA Coordinator, addresses PA records disposition, addresses PA processing procedures, identifies those PA systems of records being used by their activity; and provide training/ guidance to those personnel involved with collecting, maintaining, disseminating information from a PA system of records.

(8) Review internal directives, forms, practices, and procedures, including those having PA implications and where PA Statements (PAS) are used or PPI is solicited.

(9) Maintain liaison with records management officials (e.g., maintenance and disposal procedures and standards, forms, and reports), as appropriate.

(10) Provide guidance on handling PA requests; scope of PA exemptions; and the fees, if any, that may be collected.

(11) Conduct staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the PA.

(12) Work closely with their PA systems managers to ensure they are properly trained with regard to collecting, maintaining, and disseminating information in a PA system of records notice.

(13) Process PA complaints.

(14) Ensure protocols are in place to avoid instances of loss of PPI. Should a loss occur, take immediate action to apprise affected individuals of how to ensure their identity has not been compromised.

(15) Work closely with their public affairs officer and/or web master to ensure that PPI is not placed on public web sites or in public folders.

(16) Annually conduct reviews of their PA systems of records to ensure that they are necessary, accurate and complete.

(17) Provide CNO (DNS-36) or CMC (ARSF) respectively, with a complete listing of all PA Coordinators under their jurisdiction. Such information should include activity name, complete mailing and e-mail addresses, office code, name of PA Coordinator, and commercial, DSN, and fax telephone numbers.

(18) Review and validate PIAs for their information systems and submit the validation to CNO (DNS-36) for Navy information systems or to HQMC (ARSF) for Marine Corps information systems.

i. DON Employees/Contractors. DON employees/contractors are responsible for safeguarding the rights of others by:

(1) Ensuring that PPI contained in a system of records, to which they have access or are using to conduct official

business, is protected so that the security and confidentiality of the information is preserved.

(2) Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this instruction or the specific PA systems of records notice.

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

(4) Safeguarding the privacy of individuals and confidentiality of PPI contained in a system of records.

(5) Properly marking all documents containing PPI data (e.g., letters, emails, message traffic, etc) as “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE – Any misuse or unauthorized disclosure can result in both civil and criminal penalties.”

(6) Not maintaining privacy sensitive information in public folders.

(7) Reporting any unauthorized disclosure of PPI from a system of records to the applicable Privacy POC for his/her activity.

(8) Reporting the maintenance of any unauthorized system of records to the applicable Privacy POC for his/her activity.

j. Denial Authority. Within DON, the head of the activity having cognizance over an exempt PA system of record is authorized to deny access to that information under the exemptions cited in the PA systems of records notice. The denial authority may also deny requests to amend a system of records or to deny notification that a record exists. As deemed appropriate, the head of the activity may further designate initial denial authority to an individual properly trained on the provisions of the PA and this instruction.

k. Release Authority. Within DON, officials having cognizance over a non-exempt PA system of record that is requested by a first party or his/her authorized representative are authorized to release records. A release authority may also grant requests for notification and amendment of systems of records. The PA systems manager, who is properly trained on the provisions of references (a), (b), and (c), may be delegated this responsibility.

l. Review Authority

(1) Assistant Secretary of the Navy (Manpower & Reserve Affairs) (ASN (M&RA)) is designated to act upon requests for administrative review of initial denials of requests for amendment of records related to fitness reports and performance evaluations of military personnel.

(2) Both the Judge Advocate General (JAG) and General Counsel (GC) are designated to act upon requests for administrative review of initial denials of records for notification, access, or amendment of records under their cognizance.

(3) The authority of SECNAV, as the head of an agency, to request records subject to the PA from an agency external to DOD for civil or criminal law enforcement purposes, under subsection (b)(7) of reference (a), is delegated to CMC; the Commander, Naval Criminal Investigative Service; JAG and GC.

m. System Manager. System managers are responsible for overseeing the collection, maintenance, use, and dissemination of information from a PA system of records and ensuring that all personnel who have access to those records are aware of their responsibilities for protecting PPI that is being collected or maintained. In this capacity, they shall:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction, or disclosure.

(2) Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(3) Work closely with their coordinator to ensure that all personnel who have access to a PA system of records are properly trained on their responsibilities under the PA. Training materials may be downloaded from http://www.privacy.navy.mil.

(4) Ensure that no illegal files are maintained. [Note: Official files on individuals that are retrieved by name and/or personal identifier must be approved and published in the Federal Register.]

(5) Review annually each PA system of records notice under their cognizance to determine if the records are up-to-date and/or used in matching programs and whether they are in compliance with the OMB Guidelines. Such items as organization names, titles, addresses, etc., frequently change and should be reported to CNO (DNS-36) for updating and publication in the Federal Register.

(6) Work with IT personnel to identify any new information systems being developed that contain PPI. If a PA systems notice does not exist to allow for the collection, assist in creating a new systems notice that permits collection.

(7) Complete and maintain a PIA for those systems that collect, maintain or disseminate IIF, according to DON PIA guidance found at http://www.privacy.navy.mil and http://www.doncio.navy.mil.

(8) Complete and maintain a disclosure accounting form for all disclosures made without the consent of the record subject, except those made within DOD or under FOIA. [See paragraph 14].

(9) Ensure that only those DOD/DON officials with a "need to know" in the official performance of their duties has access to information contained in a system of records.

(10) Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PPI contained in a system of records.

(11) Ensure that records are maintained in accordance with the identified PA systems of records notice.

(12) Ensure that each newly proposed PA system of records notice is evaluated for need and relevancy and confirm that no existing PA system of records notice covers the proposed collection.

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

(14) Ensure that records are kept in accordance with retention and disposal requirements set forth in reference (j).

(15) Take reasonable steps to ensure the accuracy, relevancy, timeliness, and completeness of a record before disclosing the record to anyone outside the Federal Government.

(16) Identify all systems of records that are maintained in whole or in part by contractor personnel, ensuring that they are properly trained and that they are routinely inspected for PA compliance.

8. Policy. The DON recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected and that PPI shall be collected, maintained, used, or disclosed to ensure that it is relevant and necessary to accomplish a lawful DON/DOD purpose required to be accomplished by statute or Executive Order (E.O.). Accordingly, it is DON policy that DON activities shall fully comply with references (a), (b), and (c) to protect individuals from unwarranted invasions of privacy when information is collected, processed, maintained, or disseminated. To ensure compliance, DON activities shall:

a. Collection, Maintenance and Use

(1) Only maintain systems of records that have been approved and published in the Federal Register. See http://www.privacy.navy.mil for a list of all DOD, Navy, Marine Corps, and component systems of records notices, as well as, links to government-wide systems that the DON is eligible to use). [Note: CNO (DNS-36) can assist Navy activities in identifying existing systems that may meet their needs and HQMC (ARSF) can assist Marine Corps activities.]

(2) Only collect, maintain, and use PPI needed to support a DON function or program as authorized by law or E.O. and disclose this information only as authorized by reference (a) and this instruction. In assessing need, DON activities shall consider alternatives such as: truncating the Social Security Number (SSN) by only using the last four digits; using information that is not individually identifiable; using a sampling of certain data for certain individuals only. Additionally, they shall consider the length of time the information is needed and the cost of maintaining the information compared to the risks and adverse consequences of not maintaining the information.

(3) Only maintain PPI that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(4) DON activities shall not maintain records describing how an individual exercises his/her rights guaranteed by the First Amendment (freedom of religion; freedom of political beliefs; freedom of speech; freedom of the press; the right to peaceful assemblage; and petition for redress of grievances), unless they are: expressly authorized by statute; authorized by the individual; within the scope of an authorized law enforcement activity; or are used for the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains. [Note: This should not be construed, however, as restricting or excluding solicitation of information that the individual is willing to have in his/her record concerning religious preference, particularly that required in emergency situations.]

b. Disposal. Dispose of records from systems of records to prevent inadvertent disclosure. To this end:

(1) Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) DON activities may recycle PA data. Such recycling must be accomplished to ensure that PPI is not compromised. Accordingly, the transfer of large volumes of records in bulk to an authorized disposal activity is not considered a disclosure of records.

(3) When disposing of or destroying large quantities of records from a system of records, DON activities must ensure that the records are disposed of to preclude easy identification of specific records.

c. Individual Access

(1) Allow individuals to have access to and/or copies of all or portions of their records to which they are entitled. In the case of a legal guardian or custodial parent of a minor, they have the same rights as the individual he/she represents. A minor is defined as an individual under the age of 18. In the

case of members of the Armed Forces under the age of 18, they are not considered to be minors for the purposes of the PA.]

(2) Enter all PA first-party access requests into a tracking system and assign a case file number. [Files should comply with DON PA systems of records notice NM05211-1, PA Request Files and Tracking System at http://www.privacy.navy.mil/notices.]

(3) Allow individuals to seek amendment of their records when they can identify and provide proof that factual information contained therein is erroneous, untimely, incomplete, or irrelevant. While opinions are not subject to amendment, individuals who are denied access to amending their record may have a statement of disagreement added to the file.

(4) Allow individuals to appeal decisions that deny them access to or refusal to amend their records. If a request to amend their record is denied, allow the individual to file a written statement of disagreement.

d. Posting and Use of PA Sensitive Information

(1) Do not post PPI on an Internet site. Also, limit the posting and use of PA sensitive information on an Intranet web site, letter, fax, email, etc.

(2) When posting or transmitting PPI, ensure the following legend is posted on the document: FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."

e. Safeguarding PPI. DON activities shall establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats of hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept. At a minimum, DON activities shall:

(1) Tailor system safeguards to conform to the type of records in the system, the sensitivity of the PPI stored, the storage medium used, and the number of records maintained.

(2) Treat all unclassified records that contain PPI that normally would be withheld from the public under FOIA exemptions (b)(6) and (b)(7)(C) as if they were designated “For Official Use Only” and safeguard them from unauthorized disclosure.

(3) Ensure that privacy considerations are addressed in the reengineering of business processes and take proactive steps to ensure compliance with the PA and reference (a) as they move from conducting routine business via paper to electronic media.

(4) Recognize the importance of protecting the privacy of its members, especially as it modernizes its collection systems. Privacy issues must be addressed when systems are being developed, and privacy protections must be integrated into the development life cycle of automated systems. This applies also to contractors, vendors, and other entities that develop, procure, or use IT systems under contract to DOD/DON, to collect, maintain, or disseminate IIF from or about members of the public [see paragraph 18.]

(5) Ensure that adequate safeguards are implemented and enforced to prevent misuse, unauthorized disclosure, alteration, or destruction of PPI in records per reference (a) and this instruction.

9. Collecting Information About Individuals

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

b. Collecting Information About Individuals from Third Persons. It may not always be practical to collect all information about an individual directly. For example, when verifying information through other sources for security or employment suitability determinations; seeking other opinions, such as a supervisor’s comments on past performance or other evaluations; obtaining the necessary information directly from the individual would be exceptionally difficulty or would result in unreasonable costs or delays; or, the individual requests or consents to contacting another person to obtain the information.

c. Soliciting the SSN

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

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

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

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

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

(6) DON activities are discouraged from collecting SSNs when another identifier would suffice. In those instances where activities wish to differentiate individuals, they may find it advantageous to only collect the last four digits of the individual's SSN, which is not considered to be privacy sensitive.

(7) If a DON activity requests an individual's SSN even though it is not required by Federal statute, or is not for a system of records in existence and operating prior to 1 January 1975, it must provide a PAS and make it clear that disclosure of the number is voluntary. Should the individual refuse to disclose his/her SSN, the activity must be prepared to identify the individual by alternate means.

d. Contents of a PAS

(1) When an individual is requested to furnish PPI for possible inclusion in a system of records, a PAS must be provided to the individual, regardless of the method used to collect the information (e.g., forms, personal or telephonic interview, etc). If the information requested will not be included in a system of records, a PAS is not required.

(2) The PAS shall include the following:

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

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

(c) The principal purposes for collecting the information;

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

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

(3) The PAS must appear on the form used to collect the information or on a separate form that can be retained by the individual collecting the information. If the information is collected by a means other than a form completed by the

individual, i.e., solicited over the telephone, the PAS should be read to the individual and if requested by the individual, a copy sent to him/her. There is no requirement that the individual sign the PAS.

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

(1) Immediately below the title of the form;

(2) Elsewhere on the front page of the form (clearly indicating it is the PAS);

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

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

f. Using Forms Issued by Non-DOD Activities. Forms subject to the PA issued by other Federal agencies have a PAS attached or included. DON activities shall ensure that the statement prepared by the originating agency is adequate for the purpose for which the form will be used by the DON activity. If the PAS provided is inadequate, the DON activity concerned shall prepare a new statement or a supplement to the existing statement before using the form. Forms issued by agencies not subject to the PA (state, municipal, and local agencies) do not contain a PAS. Before using a form prepared by such agencies to collect PPI subject to this instruction, as appropriate PAS must be added.

10. Record Access. The access provisions of this instruction are intended for use by individuals about whom records are maintained in systems of records. Accordingly, only individuals seeking first party access to records retrieved by their name and/or personal identifier from a system of records have access under the provisions of reference (a) and this instruction, unless they provide written authorization for their representative to act on their behalf. [See paragraph 10f regarding access by custodial parents and legal guardians.]

a. How to Request Records. Individuals shall address requests for access to records retrieved by their name and/or personal identifier to the PA systems manager or to the office designated in the paragraph entitled, “Record Access Procedures.”

(1) DON activities may not require an individual to state a reason or justify the need to gain access under reference (a) of this instruction.

(2) However, an individual must comply with the requirements of the PA and this instruction in order to seek access to records under the provisions of reference (a) and this instruction. Specifically, individuals seeking access to records about themselves that are maintained in a PA system of records must sign their request and provide specific identifying data to enable a search for the requested record. Failure to sign the request or to provide sufficient identifying data to locate the record will result in the request being returned for non-compliance with the "Record Access Procedures" cited in the PA system of records notice.

b. Authorized Access

(1) Individuals may authorize the release of all or part of their records to anyone they choose provided they submit a signed authorization to that DON activity. Such authorization must specifically state the records to which the individual may have access.

(2) Individuals may be accompanied by anyone they choose when seeking to review their records. In such instance, DON activities shall require the individual to provide a written authorization to allow the record to be discussed in front of the other person.

c. Failure to Comply. First party requesters will be granted access to their records under the provisions of the PA, unless:

(1) they did not properly identify the records being sought; did not sign their request; and/or failed to provide sufficient identifying data to locate the requested record(s);

(2) they are seeking access to information in a system of records that is exempt from disclosure in whole or in part under the provisions of reference (a);

(3) they are seeking access to information that was compiled in anticipation of a civil action or proceeding [i.e., (d)(5) applies.] The term "civil action or proceeding" includes quasi-judicial and pre–trial judicial proceedings, as well as formal litigation. However, this does not prohibit access to

records compiled or used for purposes other than litigation or to records frequently subject to litigation. The information must have been compiled for the primary purpose of litigation to be withheld under 5 U.S.C. 552a(d)(5); or

(4) they are seeking access to information contained in the system that is currently and properly classified [see 5 U.S.C. 552a(k)(1)];

d. Blanket Requests. Many DON activities are unable to respond to "blanket" requests from individuals for access or copies of "all records pertaining to them," because they do not have a centralized index that would allow them to query by name and personal identifier to identify "all files." Accordingly, it is the requester's responsibility to identify the specific PA system of records notice for which they seek information. To assist the requester in identifying such systems, DON activities shall apprise the requester that a listing of all DON PA systems of records can be downloaded from http://www.privacy.navy.mil and that they should identify the specific records they are seeking and write directly to the PA systems manager listed in the notice, following the guidance set forth under the section entitled "Record Access Procedures" of the notice.

e. Access by Custodial Parents and Legal Guardians. The custodial parent of any minor, or the legal guardian of any individual declared by a court of competent jurisdiction to be incompetent due to physical or mental incapacity or age, may obtain access to the record of the minor or incompetent individual under the provisions of the PA, if they are acting on behalf of/in the best interest of/for the benefit of the minor or incompetent. If the systems manager determines that they are not acting on behalf of/in the best interest of/for the benefit of the minor or incompetent, access will not be granted under the PA and the request will be processed under FOIA [reference (e).] See paragraph 23c regarding access to medical records.

f. Access by a Minor or Incompetent. The right of access of the parent or legal guardian is in addition to that of the minor or incompetent. Although a minor or incompetent has the same right of access as any other individual under this instruction, DON activities may wish to ascertain whether or not the individual is being coerced to obtain records for the benefit of another. If so, the activity may refuse to process the request under the provisions of PA.

g. Requests from Members of Congress. Requests received from a Member of Congress on behalf of a constituent shall be processed under the provisions of the PA and this instruction if the requester is seeking access to records about the constituent contained in a non-exempt PA system of records (i.e., first party request). Otherwise, the request will be processed under the provisions of the FOIA [see reference (e)] since the request is received from a third party (i.e., not the record subject).

(1) The DOD "Blanket Routine Uses" enables DON activities to process requests from Members of Congress on behalf of their constituents without submitting a written authorization from the constituent granting authorization to act on their behalf.

(2) In those instances where the DON activity wishes to verify that a constituent is seeking assistance from a Member of Congress, an oral or written statement by a Congressional staff member is sufficient to confirm that the request was received from the individual to whom the record pertains.

(3) If the constituent inquiry is made on behalf of an individual other than the record subject (i.e., a third party requester), advise the Member of Congress that a written consent from the record subject is required before information may be disclosed. Do not contact the record subject to obtain consent for the disclosure to the Member of Congress, unless specifically requested by the Member of Congress.

(4) Depending on the sensitivity of the information being requested, a DON activity may choose to provide the record directly to the constituent and notify the congressional office that this has been done without providing the record to the congressional member.

h. Release of PPI. Release of PPI to individuals under the PA and/or this instruction is not considered to be a public release of information.

i. Verification of Identity

(1) An individual shall provide reasonable verification of identity before obtaining access to records. In the case of seeking to review a record in person, identification of the individual can be verified by documents they normally carry (e.g., identification card, driver's license, or other license, permit/pass). DON activities shall not, however, deny access to

an individual who is the subject of the record solely for refusing to divulge his/her SSN, unless it is the only means of retrieving the record or verifying identity.

(2) DON activities may not insist that a requester submit a notarized signature to request records. Instead, the requester shall be offered the alternative of submitting 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."

j. Telephonic Requests. DON activities shall not honor telephonic requests nor unsigned email/fax/letter requests for first party access to a PA system of records.

k. Denials

(1) An individual may be denied access to a record pertaining to him/her only if the record was compiled in reasonable anticipation of civil action; is in a system of records that has been exempted from the access provisions of this instruction under one of the permitted exemptions; contains classified information that has been exempted from the access provision of this instruction under the blanket exemption for such material claimed for all DOD PA systems of records; is contained in a system of records for which access may be denied based on some other federal statute.

(2) Only deny the individual access to those portions of the records for which the denial of access serves some legitimate governmental purpose.

(3) Only a designated denial authority may deny access to information contained in an exempt PA system of records. The denial must be in writing and at a minimum include the name, title or position and signature of the designated denial authority; the date of the denial; the specific reason for the denial, including specific citation to the appropriate sections of the PA or other statutes, this instruction, or CFR authorizing the denial; notice to the individual of his/her right to appeal the denial through the component appeal procedure within 60 calendar days; and, the title or position and address of the PA appeals official for the DON.

l. Illegible or Incomplete Records. DON activities may not deny an individual access to a record solely because the physical condition or format of the record does not make it

readily available (i.e., when the record is in a deteriorated state or on magnetic tape). DON activities may either prepare an extract or recopy the document and mark it "Best Copy Available."

m. Personal Notes

(1) Certain documents under the physical control of a DON employee and used to assist him/her in performing official functions are not considered "agency records" within the meaning of this instruction. Un-circulated personal notes and records that are not disseminated or circulated to any person or organization (e.g., personal telephone lists or memory aids) that are retained or discarded at the author's discretion and over which the DON activity does not exercise direct control, are not considered "agency records." However, if personnel are officially directed or encouraged, either in writing or orally, to maintain such records, they may become "agency records," and may be subject to this instruction.

(2) The personal un-circulated handwritten notes of unit leaders, office supervisors, or military supervisory personnel concerning subordinates are not systems of records within the meaning of this instruction. Such notes are an extension of the individual's memory. These notes, however, must be maintained and discarded at the discretion of the individual supervisor and not circulated to others. Any established requirement to maintain such notes (such as, written or oral directives, regulations, or command policy) make these notes "agency records" and they then must be made a part of a system of records. If the notes are circulated, they must be made a part of a system of records. Any action that gives personal notes the appearance of official agency records is prohibited, unless the notes have been incorporated into a system of records.

n. Compiled in Anticipation of Litigation. An individual is not entitled to access information compiled in reasonable anticipation of a civil action or proceeding. Accordingly, deny access under 5 U.S.C. 552a(d)(5) and then process under FOIA [reference (f)] to determine releasibility.

11. Amendment of Records. Amendments under this instruction are limited to correcting factual or historical matters (i.e., dates and locations of service, participation in certain actions of activities, not matters of opinion (e.g., evaluations of work performance and assessments of promotion potential contained in employee evaluations, fitness reports, performance appraisals,

or similar documents) except when such matters of opinion are based solely on inaccurate facts and the accuracy of those facts has been thoroughly discredited.

a. Individual Review and Correction. Individuals are encouraged to make periodic reviews of the information maintained about them in systems of records and to avail themselves of the amendment procedures established by reference (a), this instruction, and other regulations to update their records.

b. Eligibility. An individual may request amendment of a record retrieved by his/her personal identifier from a system of records, unless the:

(1) system has been exempt from the amendment procedure under reference (a) and/or

(2) record is covered by another procedure for correction, such as by the Board for Correction of Naval Records.

c. Amendment Requests. Amendment requests shall be in writing, except for routine administrative changes, such as change of address.

(1) An amendment request must include: a description of the factual or historical information to be amended; the reason for the amendment; the type of amendment action sought (e.g., deletion, correction, or addition); and copies of available documentary evidence that support the request.

(2) The burden of proof rests with the individual. The individual must demonstrate the existence of specific evidence establishing the factual or historical inaccuracy, and in the case of matters of opinion, must specifically discredit the underlying facts. General allegations of error are inadequate.

(3) The individual may be required to provide identification to prevent the inadvertent or intentional amendment of another’s record.

d. Limits on Attacking Evidence Previously Submitted

(1) The amendment process is not intended to permit the alteration of evidence presented in the course of judicial or quasi-judicial proceedings. Any amendments or changes to these

records normally are made through the specific procedures established for the amendment of such records.

(2) Nothing in the amendment process is intended or designed to permit a collateral attack upon what has already been the subject of a judicial or quasi-judicial determination. However, while the individual may not attack the accuracy of the judicial or quasi-judicial determination under this instruction, he/she may challenge the accuracy of the recording of that action.

e. Sufficiency of a Request to Amend. DON activities shall consider the following factors when evaluating the sufficiency of a request to amend: the accuracy of the information itself and the relevance, timeliness, completeness, and necessity of the recorded information for accomplishing an assigned mission or purpose.

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

g. Granting an Amendment Request in Whole or in Part. A record must be accurate, relevant, timely, complete, and necessary. If the record in its present state does not meet each of the criteria, the requester’s request to amend the record should be granted to the extent necessary to meet them.

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

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

agencies be notified, provide the notification of amendment even if those activities or agencies are not listed on the disclosure accounting form.

h. Denying an Amendment Request. If an amendment request is denied in whole or in part, promptly notify the individual in writing and include the following information in the notification:

(1) those sections of reference (a) or this instruction upon which the denial is based;

(2) his/her right to appeal to the head of the activity for an independent review of the initial denial;

(3) the procedures for requesting an appeal, including the title and address of the official to whom the appeal should be sent; and

(4) where the individual can receive assistance in filing the appeal.

i. Requests for Amendment of OPM Records. The records in an OPM government-wide system of records are only temporarily in the custody of DON activities. See the appropriate OPM Government-wide systems notice at http://www.defenselink.mil/privacy/govwide for guidance on how to seek an amendment of information. The custodian DON denial authority may deny a request, but all denials are subject to review by the Assistant Director for Workforce Information, Office of Merit Systems Oversight and Effectiveness, Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415.

j. Individual's Statement of Disagreement

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

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

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

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

k. Statement of Reasons

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

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

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

12. PA Appeals

a. How to File an Appeal. Individuals wishing to appeal a denial of notification, access, or amendment of records shall follow these guidelines:

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

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

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

c. Review Authorities. ASN (M&RA), JAG, and GC are authorized to adjudicate appeals made to SECNAV. JAG and GC are

further authorized to delegate this authority to a designated Assistant JAG or Deputy Assistant JAG and the Principal Deputy General Counsel or Deputy General Counsel, respectively, under such terms and conditions as they deem appropriate.

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

(2) If the record pertains to the employment of a present or former Navy or Marine Corps civilian employee, such as Navy or Marine Corps civilian personnel records or an employee's grievance or appeal file, send it to the General Counsel of the Navy, 1000 Navy Pentagon, Washington, DC 20350-1000.

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

(4) All other records dealing with present or former military members should be sent to the Office of the Judge Advocate General, 1322 Patterson Avenue SE, Suite 3000, Washington Navy Yard, DC 20374-5066.

d. Appeal Procedures

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

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

e. Final Action, Time Limits and Documentation

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

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

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

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

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

13. Conditions of Disclosure. The PA identifies 12 conditions of disclosure whereby records contained in a system of records may be disclosed by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. These instances are identified as:

a. Official Need to Know. Records pertaining to an individual may be disclosed without the consent of the individual to any DOD official who has need for the record in the performance of his/her assigned duties. Rank, position, or title alone does not authorize access to PPI about others. An official need must exist before disclosure can be made. For the purposes of disclosure, DOD is considered a single agency. Note: No disclosure accounting required.

b. FOIA. Records must be disclosed if their release is required by FOIA. References (e) and (f) require that records be made available to the public unless exempted from disclosure by one of the nine FOIA exemptions found in the Act. It follows, therefore, that if a record is not exempt from disclosure, it must be released. Note: No disclosure accounting required.

c. Routine Use. Each DON PA system of records notice identifies what records may be disclosed outside DOD without consent of the individual to whom the record pertains. Note: Disclosure accounting is required.

(1) A routine use shall be compatible with and related to the purpose for which the record was compiled; identify the persons or organizations to whom the record may be released; identify specifically the uses to which the information may be put by the receiving agency; and, have been published previously in the Federal Register.

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

(3) A routine use may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the Federal Register for at least 30 days before actually disclosing the records.

(4) In addition to specific routine uses, the DOD has identified certain “Blanket Routine Uses” that apply to all systems, unless the systems notice states that they do not. See paragraph (15) regarding Blanket Routine Uses.

d. Bureau of Census. Records may be disclosed to the Bureau of Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13. Note: Disclosure accounting is required.

e. Statistical Research and Reporting. Records may be disclosed for statistical research and reporting without the consent of the individual to whom they pertain. Before such disclosures, the recipient must provide advance written assurance that the records will be used as statistical research or reporting records; only to transferred in a form that is not individually identifiable; and will not be used, in whole or in part, to make any determination about rights, benefits, or entitlements of specific individuals. Note: Disclosure accounting is required.

f. National Archives and Records Administration (NARA). Records may be disclosed to NARA as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for evaluation by the Archivist of

the U.S. or his designee to determine whether the record has such value. Note: Disclosure accounting is required.

(1) Records may be disclosed to NARA to carry out records management inspections required by law.

(2) Records transferred to a Federal Records Center (FRC) operated by NARA for storage are not within this category. Those records continue to be maintained and controlled by the transferring DON activity. The FRC is considered to be the agency of the DON for this purpose.

g. Disclosures for Law Enforcement Purposes. Records may be disclosed without the consent of the individual whom they pertain to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity provided the civil or criminal law enforcement activity is authorized by law; the head of the law enforcement activity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigations, enforcement of a civil law, or a similar purpose) for which the record is sought; and there is no federal statute that prohibits the disclosure of the records to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

(1) Disclosure to foreign law enforcement agencies is not governed by the provisions of reference (a). To enable disclosure, a specific routine use must be published in the record system notice or another governing authority must exist.

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

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

(4) When a record is released to a law enforcement activity under this routine use, DON activities shall maintain a disclosure accounting. This disclosure accounting shall not be

made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be released.

(5) The Blanket Routine Use for law enforcement records applies to all DON PA systems of records notices. Only by including this routine use can a DON activity on its own initiative report indications of violations of law found in a system of records to a law enforcement activity without the consent of the individual to whom the record pertains.

h. Emergency Disclosures. Records may be disclosed without the written consent of the individual to whom they pertain if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the record disclosed. Note: Disclosure accounting is required.

(1) When such a disclosure is made, notify the individual who is the subject of the record. Notification sent to the last known address of the individual reflected in the records is sufficient.

(2) In instances where information is requested by telephone, an attempt will be made to verify the enquirer's and medical facility's identities and the caller's telephone number.

(3) The specific data to be disclosed is at the discretion of the releasing authority. Emergency medical information may be released by telephone.

i. Disclosure to Congress

(1) Records may be disclosed without the consent of the individual to whom they pertain to either house of the Congress or to any committee, joint committee or subcommittee of Congress if the release pertains to a matter within the jurisdiction of the committee. Note: Disclosure accounting is required.

(2) See paragraph 10g regarding how to process constituent inquiry requests.

j. Government Accountability Office (GAO). Records may be disclosed to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the GAO. Note: Disclosure accounting is required.

k. Court Orders. Records may be disclosed without the consent of the person to who they pertain under a court order signed by a judge of a court of competent jurisdiction. Releases may also be made under the compulsory legal process of federal and state bodies having authority to issue such process. Note: Disclosure accounting is required.

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

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

l. Disclosures to Consumer Reporting Agencies. Certain information may be disclosed to a consumer reporting agency in accordance with section 3711(f) of Title 31. [Note: Certain information (e.g., name, address, SSN, other information necessary to establish the identity of the individual; amount, status, and history of the claim; and the agency or program under which the claim arose, may be disclosed to consumer reporting agencies (i.e., credit reference companies as defined by the Federal Claims Collection Act of 1966, 31 U.S.C. 952d).] Note: Disclosure accounting is required.

14. Disclosure Accounting. Disclosure accounting allows the individual to determine what agencies or persons have been provided information from the record, enable DON activities to advise prior recipients of the record of any subsequent amendments or statements of dispute concerning the record, and provide an audit trail of DON's compliance with reference (a). Since the characteristics of various records maintained within the DON vary widely, no uniform method for keeping disclosure accountings is prescribed. The primary criteria are that the

selected method be one which will enable an individual to ascertain what persons or agencies have received disclosures pertaining to him/her; provide a basis for informing recipients of subsequent amendments or statements or dispute concerning the record; and, provide a means to prove, if necessary, that the activity has complied with the requirements of reference (a) and this instruction.

a. Record of Disclosures Made. DON activities must keep an accurate record of all disclosures made from a record (including those made with the consent of the individual) except those made to DOD personnel for use in performing their official duties and those disclosures made under FOIA. Accordingly, each DON activity with respect to each system of records under its control must keep a record of the date of the disclosure, a description of the information disclosed, the purpose of the disclosure, and the name and address of the person or agency to whom the disclosure was made. OPNAV Form 5211/9, Disclosure Accounting Form, is downloadable from http://www.privacy.navy.mil and should be used whenever possible to account for disclosures. [Note: DON activities do not have to maintain a disclosure accounting for disclosures made under (b)(1), to those officers and employees of an agency which maintains the record who have a need for the record in the performance of their duties or under (b)(2) – which is required under FOIA.]

b. Retention. Disclosure accountings must be kept for five years after the disclosure is made or for the life of the record, whichever is longer.

c. Right of Access. The record subject has the right of access to the disclosure accounting except when the disclosure was made at the request of a civil or criminal law enforcement agency or when the system of records has been exempted from the requirement to provide access to the disclosure accounting.

d. Correction. A DON activity must inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of reference (a) of any record that has been disclosed to the person or agency if an accounting of the disclosure was made. The exception is for intra-agency "need to know" and FOIA disclosures.

e. Accurate Accounting. A DON activity that does not keep a running tabulation of every disclosure at the time it is made, must be able to reconstruct an accurate and complete accounting

of disclosures to be able to respond to requests in a timely fashion.

15. "Blanket Routine Uses." In the interest of simplicity, economy, and to avoid redundancy, DOD has established "DOD Blanket Routine Uses." These "blanket routine uses" are applicable to every PA system of records notice maintained within DOD, unless specifically stated within a particular systems notice. "DOD Blanket Routine Uses" are downloadable from http://www.privacy.navy.mil (Notices).

16. PA Exemptions

a. Exempt Systems of Records. Reference (a) authorizes SECNAV to adopt rules designating eligible systems of records as exempt from certain requirements of the Act. This authorization has been delegated to CNO (DNS-36), who will be responsible for proposing an exemption rule. Exempt systems of records are identified at http://www.privacy.navy.mil.

b. Exemption Rule. No PA exemption may be established for a system of records until the system itself has been established by publishing a notice in the Federal Register. This allows interested persons an opportunity to comment.

c. Access. A PA exemption may not be used to deny an individual access to information that he/she can obtain under reference (e).

d. Exemption Status. An exempt system of record that is filed in a non-exempt system of records retains its exempt status.

e. Types of Exemptions. There are two types of exemptions permitted by reference (a), general exemptions and specific exemptions.

(1) General exemptions allow a system of records to be exempt from all but specifically identified provisions of reference (a). They are:

(a) "(j)(1)" – this exemption is only available for use by CIA to protect access to their records.

(b) "(j)(2)" – this exemption protects criminal law enforcement records maintained by the DON. To be eligible, the system of records must be maintained by a DON activity that

performs, as one of its principal functions, the enforcement of criminal laws. For example, the Naval Criminal Investigative Service and military police activities qualify for this exemption. Criminal law enforcement includes police efforts to detect, prevent, control, or reduce crime, or to apprehend criminals and the activities of prosecution, court, correctional, probation, pardon, or parole authorities.

1 This exemption applies to information compiled for the purpose of identifying criminal offenders and alleged criminal offenders and identifying data and notations of arrests; the nature and disposition of criminal charges; and sentencing, confinement, release, parole and probation status; information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with the identifiable individual; and reports identifiable to an individual, compiled at any stage of the enforcement process, from arrest, apprehension, indictment, or preferral of charges through final release from the supervision that resulted from the commission of a crime.

2 The exemption does not apply to investigative records maintained by a DON activity having no criminal law enforcement duties as one of its principle functions; or investigative records compiled by any element concerning an individual's suitability, eligibility; or, qualification for duty, employment, or access to classified information, regardless of the principle functions of the DON activity that compiled them.

(2) Specific exemptions permit certain categories of records to be exempted from specific provisions of reference (a). They are:

(a) "(k)(1)": Information which is properly classified under E.O. in the interest of national defense or foreign policy. [Note: All DOD systems of records that contain classified information automatically qualify for (k)(1) exemption, without establishing an exemption rule.]

(b) "(k)(2)": Investigatory material compiled for law enforcement purposes, other than material within the scope of exemption (j)(2). If an individual is denied any right, privilege, or benefit that he would otherwise be eligible, as a result of such material, such material shall be provided to such individual, except to the extent that the disclosure would reveal the identity of a source who furnished information to the

Government under an express promise that the identity of the source would be held in confidence, or, prior to 27 September 1975 under an implied promise that the identity of the source would be held in confidence.

(c) "(k)(3)": Information maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18.

(d) "(k)(4)": Information required by statute to be maintained and used solely as statistical records.

(e) "(k)(5)": Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to 27 September 1975 under an implied promise that the identity of the source would be held in confidence.

(f) "(k)(6)": Testing and evaluation 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.

(g) "(k)(7)": Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of the source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to 27 September 1975 under an implied promise that the identity of the source would be held in confidence.

f. Detailed Analysis of PA Exemptions. A detailed analysis of each exemption can be found in the Department of Justice's (DOJ's) "Freedom of Information Act Guide & Privacy Act Overview" that appears on http://www.privacy.navy.mil.

17. PA Enforcement Actions

a. Administrative Remedies. Any individual who alleges that he/she has been affected adversely by a DON activity's violation of reference (a) and this instruction may seek relief from SECNAV through administrative channels. It is recommended that the individual first address the issue through the PA coordinator having cognizance over the relevant records or supervisor (if a Government employee). If the complaint is not adequately addressed, the individual may contact CNO (DNS-36) or CMC (ARSF), for assistance.

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

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

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

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

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

c. Civil Remedies. In addition to specific remedial actions, reference (a) provides for the payment of damages, court costs, and attorney fees in some cases.

d. Criminal Penalties. Reference (a) authorizes criminal penalties against individuals for violations of its provisions, each punishable by fines up to $5,000.

(1) Wrongful disclosure. Any member or employee of DON who, by virtue of his/her employment or position, has possession

of or access to records and willfully makes a disclosure knowing that disclosure is in violation of reference (a) or this instruction.

(2) Maintaining Unauthorized Records. Any member or employee of DON who willfully maintains a system of records for which a notice has not been approved and published in the Federal Register.

(3) Wrongful Requesting or Obtaining Records. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses.

e. Litigation Notification. Whenever a complaint citing the PA is filed in a U.S. District Court against the DON or any DON employee, the responsible DON activity shall promptly apprise CNO (DNS-36)) and provide a copy of all relevant documents. CNO (DNS-36) will in turn apprise the DPO, who will apprise the DOJ. When a court renders a formal opinion or judgment, copies of the judgment and/or opinion shall be promptly provided to CNO (DNS-36). CNO (DNS-36) will apprise the DPO.

18. PPI

a. Access/Disclosure. Access to and disclosure of PPI such as SSN, date of birth, home address, home telephone number, etc., must be strictly limited to individuals with an official need to know. It is inappropriate to use PPI in group/bulk orders. Activities must take action to protect PPI from being widely disseminated. In particular, PPI shall not be posted on electronic bulletin boards because the PA strictly limits PPI access to those officers and employees of the agency with an official need to know.

b. Transmittal. In those instances where transmittal of PPI is necessary, the originator must take every step to properly mark the correspondence so that the receiver of the information is apprised of the need to properly protect the information. For example, when transmitting PPI in a paper document, fax, or email, it may be appropriate to mark it “FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.” When sending a message that contains PPI, it should be marked FOUO. It is also advisable to inform the recipient that the message should not be posted on a bulletin board. In

all cases, recipients of message traffic that contain PPI, whether marked FOUO or not, must review it prior to posting it on an electronic bulletin board.

c. Collection/Maintenance. The collection and maintenance of information retrieved by an individual's name and/or personal identifier should be performed in compliance with the appropriate PA systems of record notice [see http://www.privacy.navy.mil]. If you need to collect and maintain information retrieved by an individual's name and/or personal identifier, you must have an approved PA systems notice to cover that collection. If you are unsure as to whether a systems notice exists or not, contact the undersigned for assistance.

d. Best Practices. PA Coordinators should work closely with command officials to conduct training, evaluate what PPI can be removed from routine message traffic, review web site postings, review command electronic bulletin boards, etc., to ensure appropriate processes are in place to minimize the misuse and overuse of PPI information that could be used to commit identity theft. PA Coordinators should also ensure that their PA systems of records managers have a copy of the appropriate PA systems notice and understand PA rules. DON activities shall ensure that PPI (e.g., home address, date of birth, SSN, credit card or charge card account numbers, etc) pertaining to a Service member, civilian employee (appropriated and non-appropriated fund), military retiree, family member, or another individual affiliated with the activity (i.e., volunteer) is protected from unauthorized disclosures. To this end, DON activities shall:

(1) Notify their personnel of this policy. Address steps necessary to ensure that PPI is not compromised.

(2) Conduct and document privacy awareness training for activity personnel (e.g., military, civilian, contractor, volunteers, NAF employees, etc). Training options include: "All Hands" awareness briefing; memo to staff; formal training; circulation of brief sheet on Best Practices, etc.

(3) Examine business practices to eliminate the unnecessary collection, transmittal and posting on internet/intranet of PPI. DON activities shall reevaluate the necessity and value of including an individual's SSN and other PPI in messages, emails, and correspondence in order to conduct official business. The overuse and misuse of SSNs should be discontinued to avoid the potential for identity theft. For

example, there is no need to include an individual's SSN in a welcome aboard message. Such messages are routinely posted on command bulletin boards that are viewable by all. If a unique identifier is needed, truncate the SSN using only the last four digits.

(4) Mark all documents that contain PPI (e.g., letters, memos, emails, messages, documents faxed, etc) FOUO. Consider using a header/footer that reads: "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

(5) Train DON military members/employees who maintain PPI on their laptop computers/BlackBerrys, who telecommute, work from home, or take work home, etc., to ensure information is properly safeguarded against loss/compromise. Should a loss occur, ensure they are aware of how, what, and where to report the loss.

(6) Review existing postings on activity web sites and public folders to ensure that the PPI is removed to prevent identity theft.

(7) Remove PPI from documents prior to posting or circulating information to individuals without an "official need to know."

(8) Evaluate risks for potential compromise of PPI held in activity files, databases, etc., to ensure proper safeguards are in place to prevent unauthorized disclosures. Revise protocols as necessary.

(9) Ensure that PPI is not left out in the open or circulated to individuals not having an official need to know.

(10) Ensure that PA systems of records are properly safeguarded and that PPI is properly destroyed (http://www.privacy.navy.mil/noticenumber/noticeindex.asp).

(11) Organizations that are moving or being disestablished need to ensure they do not dispose of documents containing PPI in containers that may be subject to public access/compromise.

(12) DON activities shall build a Privacy Team to identify ways to preclude inadvertent releases of PPI.

e. Unauthorized Disclosure. In the event an unauthorized disclosure of PPI is made, DON activities shall:

(1) Take immediate action to prohibit further damage/ disclosure.

(2) Within 10 days, the DON activity shall notify all affected individuals by letter, including the specific data involved and the circumstances surrounding the incident. If the DON activity is unable to readily identify the affected individuals, a generalized notice should be sent to the potentially affected population. As part of any notification process, individuals shall be informed to visit the Federal Trade Commission's (FTC's) web site at http://www.consumer.gov/idtheft for guidance on protective actions the individual can take. A synopsis of the disclosure made, number of individuals affected, actions to be taken, should be emailed to CNO (DNS-36) with "Identity Theft Notification" in the subject line.

(3) If the DON activity is unable to comply with the notification requirements set forth in subparagraph (2) above, the activity shall immediately inform CNO (DNS-36) as to the reasons why. CNO (DNS-36) will, in turn, notify the Secretary of Defense.

(4) DON activities shall identify ways to preclude future incidents.

19. PA Systems of Records Notices Overview

a. Scope. A "system of records notice" consists of "records" that are routinely retrieved by the name, or some other personal identifier, of an individual and under the control of the DON.

b. Retrieval Practices. How a record is retrieved determines whether or not it qualifies to be a system of records. For example, records must be retrieved by a personal identifier (name, SSN, date of birth, etc) to qualify as a system of records. Accordingly, a record that contains information about an individual but IS NOT RETRIEVED by a personal identifier does not qualify as a system of records under the provisions of the PA. [Note: The "ability to retrieve" is not sufficient to warrant the establishment of a PA system of records. The requirement is retrieval by a name or personal identifier.] Should a business practice change, DON

activities shall immediately contact CNO (DNS-36) to discuss the pending change, so that the systems notice can be changed or deleted as appropriate.

c. Recordkeeping Standards. A record maintained in a system of records subject to this instruction must meet the following criteria:

(1) Be accurate. All information in the record must be factually correct.

(2) Be relevant. All information contained in the record must be related to the individual who is the record subject and must be related to a lawful purpose or mission of the DON activity maintaining the record.

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

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

(5) Be necessary. All information in the record must be needed to accomplish a mission or purpose established by Federal Law or E.0. of the President.

d. Approval. CNO (DNS-36) is the approval authority for Navy PA systems of records actions. CMC (ARSF) is the approval authority for Marine Corps PA systems of records actions. Activities wishing to create, alter, amend, or delete systems should contact CNO (DNS-36) or CMC (ARSF), respectively. Those officials will assist in electronically preparing and coordinating the documents for DOD/Congressional approval, as electronic processing is both time and cost efficient.

e. Publication in the Federal Register. Per reference (c), the DPO has responsibility for submitting all rulemaking and changes to PA system of records notices for publication in the Federal Register and Code of Federal Regulations.

20. Changes to PA Systems of Records. CNO (DNS-36) is the approval authority for Navy/DON PA systems of records actions. CMC (ARSF) is the approval authority for Marine Corps PA systems of records actions. DON activities wishing to create, alter, amend, or delete systems should contact CNO (DNS-36) or CMC

(ARSF), who will assist in electronically preparing the documents for coordination and DOD/Congressional approval.

a. Creating a New System of Records

(1) A new system of records is one for which no existing system notice has been published in the Federal Register. DON activities wishing to establish a new PA system of records notice shall contact CNO (DNS-36) [regarding Navy system of records] or CMC (ARSF) [regarding Marine Corps system of records.] These officials will assist in the preparation and approval of the notice. Once approval is obtained from DOD, the systems notice will be published in the Federal Register for comment by the public. In the case of an exempt system of records, it will also be published at 32 CFR Part 701. A listing of all DON PA systems of records notices is available at http://www.privacy.navy.mil.

(2) A DON activity may not begin collecting or maintaining PPI about individuals that is retrieved by their name and/or personal identifier until a PA system of records notice has been approved and published in the Federal Register. Failure to comply with this mandate could result in both criminal and civil penalties.

(3) In those cases where a system of records has been cancelled or deleted and it is later determined that it should be reinstated or reused, a new system notice must be prepared.

(4) DON activities wishing to create a new PA system of records must conduct a risk analysis of the proposed system to consider the sensitivity and use of the records; present and projected threats and vulnerabilities; and projected cost effectiveness of safeguards. [See paragraph 21 regarding PIAs.]

b. Altering a System of Records Notice. A systems manager shall contact CNO (DNS-36)/CMC (ARSF) to alter a PA system of records notice when there has been:

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

alteration.

(2) A change that expands the types or categories of information maintained.

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

(4) A change that adds a new routine use.

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

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

(7) A combining of record systems due to reorganization.

c. Amending a System of Records Notice. DON activities should apprise CNO (DNS-36) or CMC (ARSF) respectively when a minor change has been made to a system of records.

d. Deleting a System of Records Notice. When a system of records is discontinued, incorporated into another system, or determined to be no longer subject to this instruction, a deletion notice must be published in the Federal Register. The deletion notice shall include the system identification number, system name, and the reason for deleting it. If a system is deleted through incorporation into or merger with another system, identify the successor system in the deletion notice. Systems managers who determine that a systems notice is no longer needed should contact CNO (DNS-36)/CMC (ARSF) who will prepare the deletion notice and submit it electronically to DOD for publication in the Federal Register.

e. Numbering a System of Records Notice. Systems of records notices are identified with an “N” for a Navy system; “M” for a Marine Corps system; or an ”NM” to identify a DON-wide system, followed by the subject matter Standard Subject Identification Code (SSIC).

f. Detailed Information. Detailed information on how to write, amend, alter, or delete a PA system of records notice is contained at http://www.privacy.navy.mil.

21. Privacy, IT and PIAs

a. Development. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and storage design. This applies to all of the development methodologies and system life cycles used in the DON.

b. E-Government Act of 2002. Reference (g) directs agencies to conduct reviews of how privacy issues are considered when purchasing or creating new IT systems or when initiating new electronic collections of IIF. See reference (h) regarding DOD PIA Guidance.

c. Purpose. To ensure IIF is only acquired and maintained when necessary and the supporting IT that is being developed and used protects and preserves the privacy of the American public and to provide a means to assure compliance with applicable laws and regulations governing employee privacy. A PIA should be prepared before developing or procuring a general support system or major application that collects, maintains, or disseminates IIF from or about DON civilian or military personnel.

d. Scope. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design. During the early stages of the development of a system, both the system owner and system developer shall work together to identify, evaluate, and resolve any privacy risks. Accordingly,

(1) System owners must address what data is to be used, how the data is to be used, and who will use the data.

(2) System developers must address whether the implementation of the owner's requirements presents any threats to privacy.

e. Requirements. Before developing, modifying or establishing an automated system of records that collects, maintains, and/or disseminates IIF, DON activities shall conduct a PIA to effectively address privacy factors. Guidance is provided at http://www.doncio.navy.mil.

f. Coverage. Reference (g) mandates the preparation of a PIA either before developing or procuring IT systems that collect, maintain, or disseminate IIF from or about members of the public or initiating a new electronic collection of IIF for 10 or more persons of the public. [Note: The public DOES NOT include DON civilian or military personnel, but DOES cover family members of such personnel, retirees and their family members, and DON contractors.] A PIA should be prepared before developing, modifying, or procuring IT systems that collect, maintain, or disseminate IIF from or about members of the public or initiating a new electronic collection of IIF for 10 or more members of the public. A PIA shall also be prepared before developing, modifying or procuring a general support system or major application that collects, maintains, or disseminates IIF from or about DON civilian and military personnel.

g. PIA Not Required

(1) Legacy systems do not require completion of a PIA. However, DON CIO may request a PIA if the automation or upgrading of these systems puts the data at risk.

(2) Current operational systems do not require completion of a PIA. However, if privacy is a concern for a system the DON CIO can request that a PIA be completed. If a potential problem is identified concerning a currently operational system, the DON will use all reasonable efforts to remedy the problem.

22. Privacy and the Web. DON activities shall consult reference (i) for guidance on what may be posted on a Navy web site.

23. Processing Requests that Cite or Imply PA, FOIA, or PA/FOIA. Individuals do not always know what Act(s) to cite when requesting information. Nonetheless, it is DON policy to ensure that they receive the maximum access to information they are requesting. Accordingly, processing guidance is as follows:

a. Cite/Imply PA

(1) Individuals who cite to the PA and/or seek access to records about themselves that are contained in a PA system of records that is retrieved by their name and personal identifier, will have their request processed under the provisions of the PA.

(2) If there is no “Exemption Claimed for this System,” then the record will be released to the requester unless: it contains classified information ((k)(1) applies); was compiled in anticipation of litigation ((d)(5) applies); or contains information about another person. Although there is no “privacy” exemption under the PA, delete any information about other persons and explain in the response letter that “information not about you” was deleted from the response. There is no PA exemption to claim and no appeal rights to be given.

b. Cite/Imply FOIA

(1) Individuals who cite/imply FOIA when seeking access to records about themselves will have their request processed under PA, if the records they seek are contained in a PA system of records that is retrieved by their name and personal identifier. However, if the system of records notice contains an exemption rule, the release of information will be adjudicated using both PA and FOIA, ensuring that the individual receives the maximum amount of information allowable under the Acts.

(2) Individuals who cite/imply FOIA and seek access to records about themselves that are not contained in a PA system of records that is retrieved by their name and personal identifier will have their request processed under FOIA.

(3) Individuals who cite to the FOIA, but do not seek access to records about themselves, will have their request processed under FOIA.

c. Cite to PA and FOIA. Individuals who cite to both PA and FOIA and seek access to records contained in a PA system of record retrieved by their name and personal identifier, will have their request as follows:

(1) If the system of records does not cite to an exemption rule, does not contain classified information, or was not compiled in anticipation of litigation, the entire file is considered releasable under the PA. However, if the file contains information about another person, that information shall be withheld and the requester apprised that information about another individual has been deleted, since the information is not about them. Since no PA exemption exists for protecting privacy, no exemption rule can be cited and appeal rights do not have to be given.

(2) If the system of records does cite to a PA exemption rule, claim the exemption and process the request under the provisions of the FOIA, ensuring the requester receives the maximum release of information allowed under the Acts.

d. Processing Time Limits. DON activities shall normally acknowledge receipt of PA requests within 10 working days and respond within 30 working days.

24. Processing "Routine Use" Disclosures

a. "Routine Use" Disclosure. Individuals or organizations may seek a "routine use" disclosure of information from a DON PA system of records if the system provides for such a disclosure.

(1) The request must be in writing and state that it is being made under a "routine use" established by a specific PA system of records notice. For example: "Under the "routine use" provisions of PA systems notice N05880-1, Security Incident System, that allows release of information to individuals involved in base incidents, their insurance companies, and/or attorneys for the purpose of adjudicating a claim, I am seeking access to a copy of my vehicle accident report to submit a claim to my insurance company. Information needed to locate this record is as follows…".

(2) The individual is provided information needed to adjudicate the claim. A release authority may sign the response letter since a release of responsive information is being disclosed under a "routine use," there is no "denial" of information (i.e., PA/FOIA exemptions do not apply), and no appeal rights cited.

(3) DON activities shall retain a copy of the request and maintain a disclosure accounting of the information released. See paragraph 14.

b. Failure to Cite to a "Routine Use." Individuals or organizations that seek access to information contained in a DON PA system of records under PA/FOIA, but who have access under a "routine use" cited in the systems notice, shall be apprised of the "routine use" access and offered the opportunity to resubmit a "routine use" request, rather than having information denied under PA/FOIA. DON activities shall not make a "routine use" disclosure without having a "routine use" request.

c. Frequent “Routine Use” Requests. DON activities (e.g., security and military police offices) that routinely receive requests for information for which a “routine use” has been established should offer a “routine use” request form. This will eliminate the unnecessary burden of processing requests under PA/FOIA when the limited information being sought is available under a “routine use.”

25. Medical Records

a. Health Information Portability and Accountability Act (HIPAA)

(1) Reference (k) establishes policies and assigns responsibilities for implementation of the standards for privacy of individually identifiable health information established by HIPAA.

(2) Reference (l) prescribes the uses and disclosures of protected health information.

(3) Detailed guidance on HIPAA compliance is available from the Bureau of Medicine and Surgery's web site at http://navymedicine.med.navy.mil and from DOD at http://www.tricare.osd.mil/hipaa/.

(4) In addition to responsibilities to comply with this instruction, references (k) and (l) must also be complied with to the extent applicable. Although nothing in this instruction violates reference (k), compliance with this instruction in connection with protected health information does not necessarily satisfy all requirements of reference (l).

b. Disclosure. DON activities shall disclose medical records to the individual to whom they pertain, even if a minor, unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. Normally, this determination shall be made in consultation with a medical practitioner.

(1) Deny the individual access to his/her medical and psychological records if that access could have an adverse affect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical practitioner. If it is medically indicated that access could have an adverse mental or physical effect on the individual, provide the record to a medical practitioner named by the

individual, along with an explanation of why access without medical supervision could be harmful to the individual. In any case, do not require the named medical practitioner to request the record for the individual.

(2) If, however, the individual refuses or fails to designate a medical practitioner, access will be refused. The refusal is not considered a denial for reporting purposes under the PA.

c. Access to a Minor's Medical Records. DON activities may grant access to a minor's medical records to his/her custodial parents or legal guardians, observing the following procedures:

(1) In the United States, the laws of the state where the records are located may afford special protection to certain medical records (e.g., drug and alcohol abuse treatment and psychiatric records.) Even if the records are maintained by a military medical facility, these statutes may apply.

(2) For installations located outside the United States, the custodial parent or legal guardian of a minor shall be denied access if all of the following conditions are met: the minor at the time of the treatment or consultation was 15, 16, or 17 years old; the treatment or consultation was within a program authorized by law or regulation to provide confidentiality to the minor; the minor indicated a desire that the treatment or consultation record be handled in confidence and not disclosed to a parent or guardian; and the custodial parent or legal guardian does not have the written authorization of the minor or a valid court order granting access.

(3) All members of the military services and all married persons are not considered minors regardless of age, and the parents of these individuals do not have access to their medical records without the written consent of the individual to whom the record pertains.

26. PA Fees. The PA fee schedule is only applicable to first party requesters who are seeking access to records about themselves that are contained in a PA system of record. DON activities receiving requests under PA, FOIA, or PA/FOIA shall only charge fees that are applicable under the Act(s) in which the request is being processed.

a. PA Costs. PA fees shall include only the direct cost of reproducing the requested record. There are no fees for search,

review, or any administrative costs associated with the processing of the PA request. The cost for reproduction of documents/ microfiche will be at the same rate as that charged under the FOIA schedule (see reference (f)).

b. Fee Waiver. A requester is entitled to the first 100 pages of duplication for free.

(1) DON activities shall waive fees automatically if the direct cost for reproduction of the remaining pages is less than the minimum fee waiver threshold addressed under FOIA fees [see reference (f).]

(2) However, DON activities should not waive fees when it is determined that a requester is seeking an extension or duplication of a previous request for which he/she was already granted a waiver.

(3) Decisions to waive or reduce fees that exceed the minimum fee waiver threshold are made on a case-to-case basis.

c. PA Fee Deposits. Checks or money orders shall be made payable to the Treasurer of the United States. DON activities will forward any remittances to the Treasury Department pursuant to the Miscellaneous Receipts Act.

27. DON PA Training Program

a. Statutory Training Requirements. The PA requires each agency to establish rules of conduct for all persons involved in the design, development, operation, handling, and maintenance of any PA system of record and to train these persons with respect to these rules.

b. OMB Training Guidelines. OMB requires that agencies instruct their personnel on their roles and responsibilities for collecting, maintaining, and disseminating PA information; on agency rules and procedures for implementing the PA; and on penalties for failing to comply with these requirements. Training programs can be conducted formally (e.g., official classes/ seminars/briefings) or informally (on-the-job training).

c. DON Training Programs. To meet these training requirements, DON activities shall ensure their personnel receive PA training, as follows:

(1) Orientation training. Training that provides individuals with a basic understanding of the requirements of the PA as it applies to the individual's job performance. The training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

(2) Specialized training. Training that provides information as to the application of specific provisions of this instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this instruction. DOD requires that public affairs officials receive annual training.

(3) Management training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the PA Program.

(4) PA systems of records training. Ensure all individuals who work with a PA system of records is trained on the provisions of the PA systems of records notice and this instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this instruction.

d. Training Materials. Training materials can be downloaded from http://www.privacy.navy.mil/.

e. Customized Training. DON activities seeking customized training should contact CNO (DNS-36) and/or CMC (ARSF) for assistance in identifying appropriate training.

f. Local Training. DON activities should be prepared to report to CNO (DNS-36) and/or CMC (ARSF) training conducted and/or received on the PA, since OMB routinely requests such information from DOD.

g. Local Training Materials. DON activities that develop PA training shall provide an electronic copy to CNO (DNS-36). If appropriate, the training will be added to training materials on the PA On-line web site for use by all.

h. Refresher Training. DON activities are encouraged to conduct PA refresher training that sensitizes its personnel on how to PPI and preclude identity theft.

i. Funding for Training. Each DON activity shall fund its own PA training program.

28. PA Self Assessments/Inspections

a. Self Assessments. DON activities are encouraged to conduct annual self-assessments of their PA program. This serves to identify strengths and weaknesses and to determine training needs of personnel who work with privacy records/information. A PA self-assessment evaluation form is provided at http://www.privacy.navy.mil [Administrative Tools] for use in measuring compliance with the PA.

b. Inspections. During internal inspections, DON inspectors shall be alert for compliance with this instruction and for managerial, administrative, and operational problems associated with the implementation of the DON's PA Program.

(1) DON inspectors shall document their findings in official reports furnished to the responsible DON officials. These reports, when appropriate, shall reflect overall assets of the activity's PA program inspected, or portion thereof, identify deficiencies, irregularities, and significant problems. Also document remedial actions taken to correct problems identified.

(2) Inspection reports and follow-up reports shall be maintained in accordance with established records disposition standards [reference (j)]. These reports shall be made available to PA program officials and to CNO (DNS-36)/CMC (ARSF) respectively.

c. Retention of Reports. Retain staff visit reports and follow-up reports per established records disposition standards (see reference (j).) Retain self-assessment reports until the next self-assessment is completed. Make these reports available, upon request, to CNO (DNS-36) or CMC (ARSF).

29. Computer Matching Program. The DPO has responsibility for coordinating the approval of DOD's participation in Computer Matching agreements with other Federal, state, and local agencies.

a. Purpose. To establish or verify initial or continuing eligibility for Federal benefit programs; verify compliance with the requirements, either statutory or regulatory, of such programs; or recoup payments or delinquent debts under such Federal benefit programs.

b. Record Comparison. The record comparison must be a computerized one between two Federal Agencies or one Federal Agency and a state agency. Manual comparisons are not covered.

c. Types of Programs Not Covered

(1) State programs and programs using records about subjects who are not “individuals” as defined in are not covered.

(2) Statistical matches whose purpose is solely to produce aggregate data stripped of personal identifiers.

(3) Statistical matches whose purpose is in support of any research or statistical project.

(4) Law enforcement investigative matches whose purpose is to gather evidence against a named person or persons in an existing investigation.

(5) Tax administration matches.

(6) Routine administrative matches using Federal personnel records.

(7) Internal matches using only records from DOD systems of records.

(8) Background investigation and foreign counterintelligence matches done in the course of performing a background check for security clearances of Federal personnel or Federal contractor personnel or foreign counterintelligence.

d. Categories of Individuals Covered. Applicants for Federal benefit programs (i.e., individuals initially applying for benefits); program beneficiaries (i.e., individuals currently receiving or formerly receiving benefits); and providers of services to support such programs (i.e., those deriving income from them such as health care providers).

e. Features of a Computer Matching Program. A computer matching program entails not only the actual computerized comparison, but also preparing and executing a written agreement between the participants, securing approval of the Defense Data Integrity Board, publishing a matching notice in the Federal Register before the match begins, ensuring that investigation and due process are completed, and taking ultimate action, if any.

f. Approval/Denial of Agreements. The Executive Secretary, Defense Data Integrity Board, receives and processes for review all requests for computer matching agreements involving DOD activities. Members of the Defense Data Integrity Board are provided with a copy of the proposed computer matching agreement that details the costs associated with the match, length of agreement, and the number of computer matches expected, for their approval/disapproval.

g. Questions. CNO (DNS-36) represents the DON on the Defense Data Integrity Board. Questions from DON personnel should be directed to CNO (DNS-36).

30. Action

a. Appointments

(1) PA Coordinator. Appoint a PA Coordinator for the activity and ensure that individual is properly trained. DON activities should provide CNO (DNS-36)/CMC (ARSF) with the individual's name, activity address, email address, and telephone number within 30 days of the issuance of this instruction, ensuring that CNO (DNS-36)/CMC (ARSF) are kept apprised of any changes thereafter.

(2) PA Team. Appoint a PA Team to identify ways to ensure no inadvertent releases of PPI and establish best business practices. Membership could consist of PA systems managers, policy officials, IT professionals, records managers, public affairs officials, legal officers, etc.

b. Compliance. Take actions to ensure compliance with this instruction (e.g., conduct training; conduct PA self-assessment; review privacy protocols, conduct PIAs, etc.)

c. Implementation of Instruction. Issue a local instruction/notice/letter that implements this instruction and identifies the activity's PA Coordinator and highlights any

practices unique to the activity. There is no need to replicate this instruction.

d. PA Awareness. Ensure all personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure.

e. PA Program Updates. Routinely review http://www.privacy.navy.mil (Policies) for updates and changes to PA protocols.

f. PA Training. Ensure detailed PA training for personnel and contractors directly involved in the administration of PPI or IT systems, or with significant security responsibilities.

g. System of Records Notices. Annually review PA systems of records notices for accuracy and need (e.g., ensuring that all routine uses are necessary and complete), submitting any changes to CNO (DNS-36) or CMC (ARSF).

Dionel M. Aviles
Under Secretary of the Navy

Distribution:
Electronic only, via Navy Directives Website
http://neds.daps.dla.mil