



## DEPARTMENT OF THE NAVY

NAVY RECRUITING DISTRICT OHIO

P.O. BOX 3990

COLUMBUS, OHIO 43218-3990

IN REPLY REFER TO:

NAVCRUITDISTOHIOINST 5211.1B

10

1 8 JAN 2013

### NAVCRUITDIST OHIO INSTRUCTION 5211.1B

Subj: NAVY RECRUITING DISTRICT OHIO COMMAND PRIVACY ACT PROGRAM

Ref: (a) SECNAVINST 5211.5E  
(b) SECNAVINST 5720.42F  
(c) COMNAVCRUITCOMINST 5211.4A

1. Purpose. To implement references (a) through (c); to ensure that all NRD Ohio 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 Personally Identifiable Information (PII); 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.

2. Cancellation. NAVCRUITDISTOHIOINST 5211.1A.

3. Background. The Privacy Act (PA) of 1974, promulgated within the Department of the Navy (DON) by reference (a), is designed primarily to protect the personal privacy of individuals about whom records are maintained by agencies of the Federal Government. The Freedom of Information Act (FOIA), promulgated by reference (b), is designed to make available to the public the maximum information concerning operations, activities, and administration of the DON and other Federal agencies without invading the privacy of any individual. Although the two acts have different primary objectives, they are generally complementary in nature if carefully applied.

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

### 5. Terms and Definitions

a. Information in Identifiable Form (IIF). Information in an information technology (IT) system or online collection that directly identifies an individual (e.g., name, address, social security number or other identifying code, telephone number, e-mail address, etc.) or by which 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).

b. 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.).

c. 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 the Information Assurance Manager.

d. Personally Identifiable Information (PII). Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, birth date, home address, home phone number, or biometric records.

e. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronics, 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.

f. 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 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>.

g. System Administrator. A Department Head or Special Assistant who has cognizance over any function, program, or system of records that collects, maintains, or uses protected personal information.

h. System Manager. An official, such as the Commanding Officer, 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).

i. Privacy Act (PA) System of Records. A PA system of records notice is the authority that allows you to collect, maintain, and disseminate information which is retrieved by an individual's name and personal identifier. 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>.

6. Action

a. Privacy Act Coordinator:

- (1) Serves as principal point of contact on PA matters.
- (2) Issues an implementing instruction which designates the PA Coordinator, addresses PA records disposition and PA request processing procedures, and identifies those PA systems of records being used.
- (3) Provides overview training as promulgated by CNO (DNS-36) to command personnel on the provisions of 5 U.S.C. 522a and references (a) and (c).
- (4) Provides guidance on handling PA requests; scope of PA exemptions; and the fees, if any, that may be collected, as requested.
- (5) Processes PA complaints.
- (6) Complete and maintain a disclosure accounting form for all disclosures made.

b. District Information Assurance Manager:

- (1) Provide guidance for effective assessment and utilization of privacy-related technologies.
- (2) Provide guidance to System Administrators on the conduct of PIAs and oversee NRD Ohio PII 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.

DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(3) Review all NRD Ohio PIAs prior to approval by the DON CIO.

(4) Develop and coordinate privacy policy, procedures, education, training, and awareness practices regarding NETC information systems.

(5) Ensure NRD Ohio compliance with DON web and information systems privacy requirements, including use of encryption software and implementation of prescribed privacy-related technologies.

(6) Provide input as required for inclusion in the FISMA Report.

c. Department Heads:

(1) 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.

(2) Work closely with and ensure that PA System Administrators are properly trained on their responsibilities for protecting PII being collected, maintained, and disseminated under the DON PA Program.

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

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

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

d. System Administrator:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in systems of records that are maintained or used in your area of responsibility are protected from unauthorized alteration, destruction, or disclosure. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on

whom information is maintained. Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PII contained in a system of records.

(2) Work with SysAd personnel to identify any new information systems being developed that contain PII. If a PA systems notice does not exist to allow for the collection, notify the Legal Officer who will assist in creating a new systems notice that permits collection. 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. Ensure that no illegal files are maintained.

(3) Ensure that records are kept in accordance with retention and disposal requirements set forth in reference (a) and are maintained in accordance with the identified PA systems of records notice.

(4) Work closely with the PA coordinator to ensure that all personnel who have access to a PA system of records are properly trained on their responsibilities under the PA. 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.

(5) 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.

(6) Take reasonable steps to ensure the accuracy, relevancy, timeliness, and completeness of records that may be disclosed to anyone outside the Federal Government. Stop collecting any category or item of information about individuals that is no longer justified, and when feasible remove the information from existing records.

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

(8) Complete and maintain a PIA for those systems that collect, maintain or disseminate IIF, according to Department of the Navy PIA guidance found at <http://www.privacy.navy.mil> and <http://www.doncio.navy.mil>.

(9) Notify the Legal Officer when there is a request for PA information.

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

f. Supervisors. Per reference (c), all supervisors will conduct a PII spot check three times a year using NAVPERS 5211/15(08-07) NLT 31 Dec, 30 Apr, and 31 Aug, anytime directed, and at turnover of duties. Spot check forms will be submitted to the PA Coordinator for file and keep for a period of two years.

g. All NRD Personnel (including Contractors):

(1) Ensure that PII contained in a system of records to which you have access or are using to conduct official business is protected so that the security and confidentiality of the information is preserved.

(2) Do not disclose any information contained in a system of records by any means of communication to any person or agency, except as authorized by SECNAVINST 5211.5E or the specific PA systems of records notice.

(3) Do not maintain unpublished official files that would fall under the provisions of 5 U.S.C. 552a.

(4) Safeguard the privacy of individuals and confidentiality of PII contained in systems of records.

(5) In those instances where transmittal of PII 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. Mark all documents that contain PII (e.g., letters, memos, e-mails, messages, faxes, etc.) "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

(6) Do not maintain privacy sensitive information in public folders.

(7) Report any unauthorized disclosure of PII from a system of records to the Legal Officer.

(8) Report the maintenance of any unauthorized system of records to the Legal Officer.

(9) Dispose of records from systems of records to prevent

inadvertent disclosure. Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape. Although PA data may be recycled, it must be accomplished to ensure that PII 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.

7. Processing of Privacy Act Records. Requests for Privacy Act records should be referred to the Privacy Act Coordinator for a release determination.

8. Privacy Act Team. A Privacy Act Team, consisting of the Privacy Act Coordinator, Legal Officer, Chief Administrator and Systems Administrator, will meet quarterly to identify ways to prevent inadvertent releases of PII and to establish best business practices.

9. Web Sites. All personnel (including contractors) are required to be familiar with reference (a) and are encouraged to routinely visit the Department of the Navy PA and FOIA web sites at [www.privacy.navy.mil](http://www.privacy.navy.mil) and [www.foia.navy.mil](http://www.foia.navy.mil) to learn of the most current news, developments, and guidance.



JOHN L. NGUYEN

Distribution:  
Electronic only, via  
[https://www.milsuite.mil/wiki/Portal:Navy\\_Recruiting\\_District\\_Ohio/Command\\_Directives](https://www.milsuite.mil/wiki/Portal:Navy_Recruiting_District_Ohio/Command_Directives)