DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5211.1A
00D
10 JUL 12

CNATRA INSTRUCTION 5211.1A

Subj: NAVAL AIR TRAINING COMMAND PRIVACY PROGRAM

Ref: (a) 5 U.S.C. §552a
(b) 32 CFR Part 701, Federal Register
(c) SECNAVINST 5211.5E

1. Purpose. Per references (a) through (c) and to ensure that all Naval Air Training Command (NATRACOM) military members, civilian and contractor employees are made fully aware of their rights and responsibilities under the provisions of the Privacy Act (PA). In order to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy stemming from the Department of the Navy's (DON) collection, maintenance, use, and disclosure of Protected Personal Information (PPI). Also to require privacy information 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. CNATRAINST 5211.1

3. Background. The Privacy Act (PA) of 1974, implemented within (DON) by reference (c), is primarily designed to protect the personal privacy of individuals about whom records are maintained by agencies of the Federal Government.

4. Scope. Governs the collection, safeguarding, maintenance, use, access, amendment, and dissemination of PPI 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). See paragraph 4d and 4e for information protected by the PA not in an IT or online collection.

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 and the PA Coordinator.

d. 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.

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 Administrator. A Chief of Naval Air Training (CNATRA) headquarters Department Head/Special Assistant or the Head of a NATRACOM activity who has cognizance over any function or program that collects, maintains, or uses protected personal information.

g. System Manager. An official, such as CNATRA, 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).

h. 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 associated to the individual. System notices for all PA systems of records must be published in the Federal Register, reference (b), and are also available from the Navy's Privacy Act online web site at http://www.privacy.navy.mil.

6. Action

a. CNATRA Office of Counsel (Code 00D):

(1) Is designated the Privacy Act Coordinator and serves as the principal point of contact on PA matters.

(2) Issues implementing instructions which addresses PA records disposition, PA request processing procedures, and identifies those PA systems of records being used by CNATRA activities.

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

(4) Provides CNO (DSN-36) with a complete listing of all PA Points of Contact (POC) to include activity name, complete mailing and e-mail addresses, office code, commercial and DSN phone number and FAX telephone number.

(5) Provides overview training as promulgated by CNO (DSN-36) to NATRACOM personnel on the provisions of references (a) thru (c).

(6) Provides assistance 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, notifying CNO (DNS-36) promptly of the need.

(7) Provides guidance on handling PA requests; scope of PA exemptions; and the fees, if any that may be collected, as requested.

(8) Processes PA complaints.

(9) Requires that the disclosure accounting forms are made and maintained for all disclosures made.

b. CNATRA (N6) Information Office/Information Assurance Manager:

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

(2) Provides guidance to System Administrators on the conduct of PIAs and oversee NATRACOM 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. DON CIO reserves the right to request that a PIA be completed on any system that may have privacy risks.

(3) Reviews all NATRACOM PIAs in coordination with CNATRA PA Coordinator prior to approval by the DON Chief Information Officer.

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

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

(6) Provides input as required for inclusion in the Federal Information Management Act (FISMA) Report in coordination with CNATRA PA Coordinator.

(7) Actively explores ways to reduce the use of social security numbers in NATRACOM information systems.

c. CNATRA Department Heads/Special Assistants and NATRACOM Activity Heads:

(1) Ensure no official files that are retrieved by name or other personal identifier are maintained on individuals 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 PPI being collected, maintained, and disseminated under the DON PA Program.

(3) In coordination with CNATRA (N4), ensure contracts for the operation of a system of records specifically identify the record system and the work to be performed, and include in the solicitation and resulting contract the terms as prescribed by the Federal Acquisition Regulations (FAR), including how PPI data is to be disposed of at the end of the contract. Inform contractors of their responsibilities regarding the DON PA Program and ensure they understand PPI and comply with all protocols for handling PPI.

(4) Work closely with Public Affairs Officer and/or web master to ensure that PPI is not placed on public web sites or in public folders.

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

(6) Ensure that supervisors conduct PII spot checks of their assigned areas of responsibility on a semi-annual basis and submit documented results of the audit to 00D.

(7) Review and validate PIAs for information systems for submission to CNO (DNS-36) via CNATRA (00D).

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

d. System Administrators:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in systems of records that are maintained or used in their area of responsibility are protected from unauthorized alteration, destruction, or disclosure. Protect the records from a release of PA information that could constitute an unwarranted invasion of privacy.

(2) Work with CNATRA (N6) to identify any new information systems being developed that contain PPI. If a PA systems notice does not exist to allow for the collection, notify CNATRA (00D) who will assist in creating a new systems notice that permits collection and 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 SECNAV M-5210.1, Records Management Manual, and are maintained in accordance with the identified PA systems of records notice.

(4) Work closely with the CNATRA 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 that the records that may be disclosed or used are accurate, relevant, timely, and complete. Stop collection of 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 OMB Guidelines. Such items as organization names, titles, addresses, etc., frequently change and should be reported to CNATRA (00D) 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 DON PIA guidance found at http://www.privacy.navy.mil and http://www.doncio.navy.mil.

(9) Notify CNATRA (00D) when there is a request for PA information.

e. All NATRACOM Personnel and NATRACOM Service Contract Employees:

(1) Ensure that PPI contained in a system of records to which personnel 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.

(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 PPI contained in systems of records.

(5) 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. Mark all documents (e.g., letters, memos, e-mails, messages, faxes, etc.) that contain PPI “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 or suspected disclosure of PPI from a system of records to CNATRA (00D).

(8) Report the maintenance of any unauthorized system of records to CNATRA (00D).

(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, burying, 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 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.

(10) Completed required annual training available on NKO. Training must be completed prior to the end of August each year.

(11) Encrypted emails containing PII must have “FOUO – Privacy Sensitive” in the subject line, and attach the warning “FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.”

(12) Mark all documents that contain PII as FOUO and attached the warning “FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.”

(13) Ensure that all routed folders containing privacy information has attached a privacy cover sheet (DD Form 2923, Sep 2010).

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

8. Web Sites. All personnel (including contractors) are required to be familiar with SECNAVINST 5211.5E and are encouraged to routinely visit the DON PA and FOIA web sites at www.privacy.navy.mil and www.foia.navy.mil to learn of the most current news, developments, and guidance.

C. HOLLINGSWORTH
Chief of Staff

Distribution:
CNATRA Website