(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 5 U.S.C. 552a or any rule or regulation issued under 5 U.S.C. 552a and thereby causes the individual to be adversely affected.

(c) *Civil remedies.* In addition to specific remedial actions, 5 U.S.C. 552a provides for the payment of damages, court costs, and attorney fees in some cases.

(d) *Criminal penalties.* 5 U.S.C. 552a 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 5 U.S.C. 552a, this subpart or subpart G.

(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.

§ 701.115 Protected personal information (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 E-Mail, 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, e-mails, 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 paragraph (e)(2) of this section, 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.

§ 701.116 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 DOD 5400.11–R, the DPO has responsibility for submitting all rulemaking and changes to PA system of records notices for publication in the FEDERAL REGISTER and CFR.

§ 701.117 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