(6) DA PAM 25–51 sets forth procedures pertaining to Privacy Act system of records notices.

(7) For new systems, system managers must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. This applies to all new systems of records whether maintained manually or automated.

(i) One safeguard plan is the development and use of a Privacy Impact Assessment (PIA) mandated by the E-Gov Act of 2002, Section 208. The Office of Management and Budget specifically directs that a PIA be conducted, reviewed, and published for all new or significantly altered information in identifiable form collected from or about the members of the public. The PIA describes the appropriate administrative, technical, and physical safeguards for new automated systems. This will assist in the protection against any anticipated threats or hazards to the security or integrity of data, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. Contact your local Information Officer for guidance on conducting a PIA.

(ii) The development of appropriate safeguards must be tailored to the requirements of the system as well as other factors, such as the system environment, location, and accessibility.

§ 505.4 Collecting personal information.

(a) *General provisions.* (1) Employees will collect personal information to the greatest extent practicable directly from the subject of the record. This is especially critical, if the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs (*See* 5 U.S.C. 552a(e)(2)).

(2) It is unlawful for any Federal, State, or local government agency to deny anyone a legal right, benefit, or privilege provided by law for refusing to give their SSN unless the law requires disclosure, or a law or regulation adopted before January 1, 1975, required the SSN or if DA uses the SSN to verify a person's identity in a system of records established and in use before that date. Executive Order 9397 (issued prior to January 1, 1975) authorizes the Army to solicit and use the SSN as a numerical identifier for individuals in most federal records systems. However, the SSN should only be collected as needed to perform official duties. Executive Order 9397 does not mandate the solicitation of SSNs from Army personnel as a means of identification.

(3) Upon entrance into military service or civilian employment with DA, individuals are asked to provide their SSN. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a record, the Privacy Act Statement is not required if the individual is only requested to furnish or verify the SSN for identification purposes in connection with the normal use of his or her records. If the SSN is to be used for a purpose other than identification, the individual must be informed whether disclosure of the SSN is mandatory or voluntary; by what statutory authority the SSN is solicited; and what uses will be made of the SSN. This notification is required even if the SSN is not to be maintained in a Privacy Act system of records.

(4) When asking an individual for his or her SSN or other personal information that will be maintained in a system of records, the individual must be provided with a Privacy Act Statement.

(b) *Privacy Act Statement (PAS).* (1) A Privacy Act Statement is required whenever personal information is requested from an individual and will become part of a Privacy Act system of records. The information will be retrieved by the individual's name or other personal identifier (*See* 5 U.S.C. 552a(e)(3)).

(2) The PAS will ensure that individuals know why the information is being collected so they can make an informed decision as to providing the personal information.

(3) In addition, the PAS will include language that is explicit, easily understood, and not so lengthy as to deter an individual from reading it.

(4) A sign can be displayed in areas where people routinely furnish this kind of information, and a copy of the PAS will be made available upon request by the individual.

(5) Do not ask the person to sign the PAS.

(6) A Privacy Act Statement must include the following four items—

(i) *Authority:* Cite the specific statute or Executive Order, including a brief title or subject that authorizes the DA to collect the personal information requested.

(ii) *Principal Purpose (s):* Cite the principal purposes for which the information will be used.

(iii) *Routine Uses:* A list of where and why the information will be disclosed OUTSIDE of DOD. Applicable routine uses are published in the applicable Privacy Act system of records notice(s). If none, the language to be used is: ''Routine Use(s): None. However the 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices apply.''

(iv) *Disclosure:* Voluntary or Mandatory. Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory ONLY when a federal statute, Executive Order, regulation, or other law specifically imposes a duty on the individual to provide the information sought, and when the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of or prerequisite to granting a benefit or privilege and the individual has the option of receiving the benefit or privilege, providing the information is always voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought must be listed as a consequence of not furnishing the requested information.

(7) Some acceptable means of administering the PAS are as follows, in the order of preference—

(i) Below the title of the media used to collect the personal information. The PAS should be positioned so that the individual will be advised of the PAS before he or she provides the requested information;

(ii) Within the body with a notation of its location below the title;

(iii) On the reverse side with a notation of its location below the title;

(iv) Attached as a tear-off sheet; or

(v) Issued as a separate supplement.

(8) An example of a PAS is at appendix B of this part.

(9) Include a PAS on a Web site page if it collects information directly from an individual and is retrieved by his or her name or personal identifier (See Office of Management and Budget Privacy Act Guidelines, 40 FR 28949, 28961 (July 9, 1975)).

(10) Army policy prohibits the collection of personally identifying information on public Web sites without the express permission of the user. Requests for exceptions must be forwarded to the Army CIO/G–6. (See AR 25–1, para 6–4n.)

(c) *Collecting personal information from third parties.* (1) It may not be practical to collect personal information directly from the individual in all cases. Some examples of when collection from third parties may be necessary are when—

(i) Verifying information;

(ii) Opinions or evaluations are needed;

(iii) The subject cannot be contacted; or

(iv) At the request of the subject individual.

(2) When asking third parties to provide information about other individuals, they will be advised of—

(i) The purpose of the request; and

(ii) Their rights to confidentiality as defined by the Privacy Act of 1974 (Consult with your servicing Staff Judge Advocate for potential limitations to the confidentiality that may be offered pursuant to the Privacy Act).

(d) *Confidentiality promises.* Promises of confidentiality must be prominently annotated in the record to protect from disclosure any information provided in confidence pursuant to 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7).

§ 505.5 Individual access to personal information.

(a) *Individual access.* (1) The access provisions of this part are intended for use by individuals whose records are maintained in a Privacy Act system of