(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

records. If a representative acts on their behalf, a written authorization must be provided, with the exception of members of Congress acting on behalf of a constituent.

(2) A Department of the Army ''Blanket Routine Use'' allows the release of Privacy Act protected information to members of Congress when they are acting on behalf of the constituent and the information is filed and retrieved by the constituent's name or personal identifier. The said ''Blanket Routine Use'' is listed below.

''Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DOD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.''

(3) Upon a written request, an individual will be granted access to information pertaining to him or her that is maintained in a Privacy Act system of records, unless—

(i) The information is subject to an exemption, the system manager has invoked the exemption, and the exemption is published in the FEDERAL REGISTER; or

(ii) The information was compiled in reasonable anticipation of a civil action or proceeding.

(4) Legal guardians or parents acting on behalf of a minor child have the minor child's rights of access under this part, unless the records were created or maintained pursuant to circumstances where the interests of the minor child were adverse to the interests of the legal guardian or parent.

(5) These provisions should allow for the maximum release of information consistent with Army and DOD's statutory responsibilities.

(b) *Individual requests for access.* (1) Individuals will address requests for access to records in a Privacy Act system of records to the system manager or the custodian of the record designated in DA systems of records notices (See DA PAM 25–51 or the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy*).

(2) Individuals do not have to state a reason or justify the need to gain access to records under the Act.

(3) Release of personal information to individuals under this section is not considered a ''public release'' of information.

(c) *Verification of identity for first party requesters.* (1) Before granting access to personal data, an individual will provide reasonable verification of identity.

(2) When requesting records in writing, the preferred method of verifying identity is the submission of a notarized signature. An alternative method of verifying identity for individuals who do not have access to notary services is the submission of an un-sworn declaration in accordance with 28 U.S.C. 1746 in the following format:

(i) If executed within the United States, its territories, possessions, or commonwealths: ''I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)''.

(ii) If executed outside of the United States: ''I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).''

(3) When an individual seeks access in person, identification can be verified by documents normally carried by the individual (such as identification card, driver's license, or other license, permit or pass normally used for identification purposes). However, level of proof of identity is commensurate with the sensitivity of the records sought. For example, more proof is required to access medical records than is required to access parking records.

(4) Telephonic requests will not be honored.

(5) An individual cannot be denied access solely for refusal to provide his or her Social Security Number (SSN) unless the SSN was required for access by statute or regulation adopted prior to January 1, 1975.

(6) If an individual wishes to have his or her records released directly to a third party or to be accompanied by a third party when seeking access to his or her records, reasonable proof of authorization must be obtained. The individual may be required to furnish a

signed access authorization with a notarized signature or other proof of authenticity (*i.e.* telephonic confirmation) before granting the third party access.

(d) *Individual access to medical records.* (1) An individual must be given access to his or her medical and psychological records unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. This determination normally should be made in consultation with a medical doctor. Additional guidance is provided in DOD 5400.11–R, Department of Defense Privacy Program. In this instance, the individual will be asked to provide the name of a personal health care provider, and the records will be provided to that health care provider, along with an explanation of why access without medical supervision could be harmful to the individual.

(2) Information that may be harmful to the record subject should not be released to a designated individual unless the designee is qualified to make psychiatric or medical determinations.

(3) DA activities may offer the services of a military physician, other than the one who provided the treatment.

(4) Do not require the named health care provider to request the records for the individual.

(5) The agency's decision to furnish the records to a medical designee and not directly to the individual is not considered a denial for reporting purposes under the Act and cannot be appealed.

(6) However, no matter what the special procedures are, DA has a statutory obligation to ensure that access is provided the individual.

(7) Regardless of age, all DA military personnel and all married persons are considered adults. The parents of these individuals do not have access to their medical records without written consent of the individual.

(8) DOD 6025.18–R, DOD Health Information Privacy Regulation, issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, has placed additional procedural requirements on the uses and disclosure of individually identifiable health information beyond those found in the Privacy Act of 1974 and this part. In order to be in compliance with HIPAA, the additional guidelines and procedures will be reviewed before release of an individual's identifiable health information.

(e) *Personal notes.* (1) The Privacy Act does not apply to personal notes of individuals used as memory aids. These documents are not Privacy Act records and are not subject to this part.

(2) The five conditions for documents to be considered personal notes are as follows—

(i) Maintained and discarded solely at the discretion of the author;

(ii) Created only for the author's personal convenience and the notes are restricted to that of memory aids;

(iii) Not the result of official direction or encouragement, whether oral or written;

(iv) Not shown to others for any reason; and

(v) Not filed in agency files.

(3) Any disclosure from personal notes, either intentional or through carelessness, removes the information from the category of memory aids and the personal notes then become subject to provisions of the Act.

(f) *Denial or limitation of individual's right to access.* (1) Even if the information is filed and retrieved by an individual's name or personal identifier, his or her right to access may be denied if—

(i) The records were compiled in reasonable anticipation of a civil action or proceeding including any action where DA expects judicial or administrative adjudicatory proceedings. The term ''civil action or proceeding'' includes quasi-judicial, pre-trial judicial, and administrative proceedings, as well as formal litigation;

(ii) The information is about a third party and does not pertain to the requester. A third party's SSN and home address will be withheld. However, information about the relationship between the individual and the third party would normally be disclosed as it pertains to the individual;

(iii) The records are in a system of records that has been properly exempted by the Secretary of the Army from the access provisions of this part and the information is exempt from release

under a provision of the Freedom of Information Act (See appendix C of this part for a list of applicable Privacy Act exemptions, exceptions, and ''Blanket'' routine uses);

(iv) The records contain properly classified information that has been exempted from the access provision of this part;

(v) The records are not described well enough to enable them to be located with a reasonable amount of effort on the part of an employee familiar with the file. Requesters should reasonably describe the records they are requesting. They do not have to designate a Privacy Act system of records notice identification number, but they should at least identify a type of record or functional area. For requests that ask for ''all records about me,'' DA personnel should ask the requester for more information to narrow the scope of his or her request; and

(vi) Access is sought by an individual who fails or refuses to comply with Privacy Act established procedural requirements, included refusing to pay fees.

(2) Requesters will not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making Privacy Act requests. System managers will process such requests but inform requesters that using government resources to make Privacy Act requests is not authorized.

(3) When a request for information contained in a Privacy Act system of records is denied in whole or in part, the Denial Authority or designee shall inform the requester in writing and explain why the request for access has been refused.

(4) A request for access, notification, or amendment of a record shall be acknowledged in writing within 10 working days of receipt by the proper system manager or record custodian.

(g) *Relationship between the Privacy Act and the Freedom of Information Act.* (1) Not all requesters are knowledgeable of the appropriate statutory authority to cite when requesting information. In some instances, they may cite neither the PA nor the Freedom of Information Act in their request. In some instances they may cite one Act but not the other. The Freedom of Information Act and the PA works together to ensure that requesters receive the greatest amount of information possible.

(2) Do not deny the individual access to his or her records simply because he or she failed to cite the appropriate statute or regulation.

(3) If the records are required to be released under the Freedom of Information Act, the PA will never block disclosure to requester. If the PA allows the DA activity to deny access to an individual, the Freedom of Information Act must still be applied, and the information released if required by the Freedom of Information Act.

(4) Unlike the Freedom of Information Act, the Privacy Act applies only to U.S. citizens and aliens lawfully admitted for permanent residence.

(5) Requesters who seek records about themselves contained in a Privacy Act system of records (1st party requesters) and who cite or imply only the Privacy Act, will have their request processed under the provisions of both the PA and the Freedom of Information Act. If the information requested is not contained in a Privacy Act system of records or is not about the requester, the individual's request will be processed under the provisions of the Freedom of Information Act only, and the Freedom of Information Act processing requirements/time lines will apply.

(6) *Third party information.* (i) Third party information contained in a Privacy Act system of records that does not pertain to the requester, such as SSN, home addresses, and other purely personal information that is not about the requester, will be processed under the provisions of Freedom of Information Act only. Third party information that is not about the requester is not subject to the Privacy Act's first party access provision.

(ii) Information about the relationship between the first party requester and a third party is normally disclosed as pertaining to the first party requester. Consult your servicing Staff Judge Advocate if there is a question about the release of third party information to a first party requester.

(7) If an individual requests information about them contained in a Privacy Act system of records, the individual may be denied the information only if the information is exempt under both the PA and the Freedom of Information Act. Both PA and Freedom of Information Act exemptions will be cited in the denial letter and appeals will be processed in accordance with both Acts.

(8) Each time a first party requester cites or implies the PA, perform this analysis:

(i) Is the request from a United States living citizen or an alien lawfully admitted for permanent residence?

(ii) Is the individual requesting an agency record?

(iii) Are the records within a PA system of records that are filed and retrieved by an individual's name or other personal identifier? (If the answer is ''yes'' to all of these questions, then the records should be processed under the ''Privacy Act'') and

(iv) Does the information requested pertain exclusively to the requester?

(A) If yes, no further consideration of Freedom of Information Act exemptions required. Release all information unless a PA exemption authorizes withholding.

(B) If no, process the information that is not about the requester under the Freedom of Information Act and withhold only if a proper Freedom of Information Act exemption applies.

(h) *Functional requests.* If an individual asks for his or her records and does not cite or reasonably imply either the Privacy Act or the Freedom of Information Act, and another prescribing directive or regulation authorizes the release, the records should be released under that other directive or regulation and not the PA or the FOIA. Examples of functional requests are military members asking to see their Official Military Personnel Records or civilian employees asking to see their Official Personnel Folder.

(i) *Procedures for denying or limiting an individual's right to access or amendment and the role of the Denial Authority.* (1) The only officials authorized to deny a request for records or a request to amend records in a PA system of records pertaining to the requesting individual, are the appropriate Denial Authorities, their designees, or the Secretary of the Army who will be acting through the General Counsel.

(2) Denial Authorities are authorized to deny requests, either in whole or in part, for notification, access and amendment of Privacy Act records contained in their respective areas of responsibility.

(i) The Denial Authority may delegate all or part of their authority to a division chief under his supervision within the Agency in the grade of 0–5/GS–14 or higher. All delegations must be in writing.

(ii) The Denial Authority will send the names, office names, and telephones numbers of their delegates to the DA Freedom of Information and Privacy Office.

(iii) If a Denial Authority delegate denies access or amendment, the delegate must clearly state that he or she is acting on behalf of the Denial Authority, who must be identified by name and position in the written response to the requester. Denial Authority designation will not delay processing privacy requests/actions.

(iv) The official Denial Authorities are for records under their authority (See appendix B of this part). The individuals designated as Denial Authorities under this part are the same individuals designated as Initial Denial Authorities under AR 25–55, the Department of the Army Freedom of Information Act Program. However, delegation of Denial Authority pursuant to this part does not automatically encompass delegation of Initial Denial Authority under AR 25–55. Initial Denial Authority must be expressly delegated pursuant to AR 25–55 for an individual to take action on behalf of an Initial Denial Authority under AR 25–55.

(3) The custodian of the record will acknowledge requests for access made under the provisions of the Privacy Act within 10 working days of receipt.

(4) Requests for information recommended for denial will be forwarded to the appropriate Denial Authority, along with a copy of the records and justification for withholding the record. At the same time, notify the requester of the referral to the Denial

Authority for action. All documents or portions thereof determined to be releasable to the requester will be released to the requester before forwarding the case to the Denial Authority.

(5) Within 30 working days, the Denial Authority will provide the following notification to the requester in writing if the decision is to deny the requester access to the information.

(6) Included in the notification will be:

(i) Denying Official's name, position title, and business address;

(ii) Date of the denial;

(iii) The specific reason for the denial, citing the appropriate subsections of the Privacy Act, the Freedom of Information Act, AR 25–55, The Department of the Army Freedom of Information Act Program and this part; and

(iv) The individual's right to administratively appeal the denial within 60 calendar days of the mailing date of the notice, through the Denial Authority, to the Office of the General Counsel, Secretary of the Army, 104 Army Pentagon, Washington, DC 20310–0104.

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

(8) For denials made by the DA when the record is maintained in a Government-wide system of records, an individual's request for further review must be addressed to each of the appropriate government Privacy Act offices listed in the Privacy Act system of records notices. For a current listing of Government-wide Privacy Act system of records notices see the Defense Privacy Office's Web site *http://www.defenselink.mil/privacy* or DA PAM 25–51.

(j) *No records determinations.* (1) Since a no record response may be considered an ''adverse'' determination, the Denial Authority must make the final determination that no records exist. The originating agency shall notify the requester that an initial determination has been made that there are no responsive records, however the final determination will be made by the Denial Authority. A no records certificate must accompany a no records determination that is forwarded to the Denial Authority.

(2) The Denial Authority must provide the requester with appeal rights.

(k) *Referral of requests.* (1) A request received by a DA activity having no records responsive to a request shall be referred to another DOD Component or DA activity, if the other Component or activity confirms that they have the requested records, or verifies that they are the proper custodian for that type of record. The requester will be notified of the referral. In cases where the DA activity receiving the request has reason to believe that the existence or nonexistence of the record may in itself be classified, that activity will consult the Component or activity having cognizance over the records in question before referring the request. If the Component or activity that is consulted determines that the existence or nonexistence of the records is in itself classified, the requester shall be so notified by the DA activity originally receiving the request that it can neither confirm nor deny the existence of the record, and no referral shall take place.

(2) A DA activity shall refer a Privacy Act request for a classified record that it holds to another DOD Component, DA activity, or agency outside the Department of Defense, if the record originated in the other DOD Component, DA activity, or outside agency, or if the classification is derivative. The referring DA activity will provide the records and a release recommendation with the referral action.

(3) Any DA activity receiving a request that has been misaddressed will refer the request to the proper address and advise the requester.

(4) Within DA, referrals will be made directly to offices having custody of the requested records (unless the Denial Authority is the custodian of the requested records). If the office receiving the Privacy Act request does not know where the requested records are located, the office will contact the DA FOIA/P Office, to determine the appropriate office for referral.

(5) The requester will be informed of the referral whenever records or a portion of records are, after prior consultation, referred to another activity for a release determination and direct

response. Additionally, the DA activity referral letter will accomplish the following—

(i) Fully describe the Privacy Act system of records from which the document was retrieved; and

(ii) Indicate whether the referring activity claims any exemptions in the Privacy Act system of records notice.

(6) Within the DA, an activity will refer a Privacy Act request for records that it holds but was originated by another activity, to the originating activity for direct response. An activity will not, in any case, release or deny such records without prior consultation with the originating activity. The requester will be notified of such referral.

(7) A DA activity may refer a Privacy Act request for records that originated in an agency outside of DOD, or that is based on information obtained from an agency outside the DOD, to that agency for direct response to the requester, only if that agency is subject to the Privacy Act. Otherwise, the DA activity must respond to the request.

(8) DA activities will not honor any Privacy Act requests for investigative, intelligence, or any other type of records that are on loan to the Department of Defense for a specific purpose, if the records are restricted from further release in writing. Such requests will be referred to the agency that provided the records.

(9) A DA activity will notify requesters seeking National Security Council (NSC) or White House documents that they should write directly to the NSC or White House for such documents. DA documents in which the NSC or White House have a concurrent reviewing interest will be forwarded to the Department of Defense, Office of Freedom of Information and Security Review, which will coordinate with the NSC or White House, and return the documents to the originating DA activity after NSC or White House review. NSC or White House documents discovered in DA activity files which are responsive to a Privacy Act request will be forwarded to DOD for coordination and return with a release determination.

(10) To the extent referrals are consistent with the policies expressed above; referrals between offices of the same DA activity are authorized.

(l) *Reproduction fees.* (1) Use fees only to recoup direct reproduction costs associated with granting access.

(2) DA activities may use discretion in their decision to charge for the first copy of records provided to an individual to whom the records pertain. Thereafter, fees will be computed pursuant to the fee schedule set forth in AR 25–55, including the fee waiver provisions.

(3) Checks or money orders for fees should be made payable to the Treasurer of the United States and will be deposited in the miscellaneous receipts of the treasury account maintained at the activity's finance office.

(4) Reproduction costs shall only include the direct costs of reproduction and shall not include costs of—

(i) Time or effort devoted to searching for or reviewing the records by personnel;

(ii) Fees not associated with the actual cost of reproduction;

(iii) Producing a copy when it must be provided to the individual without cost under another regulation, directive, or law;

(iv) Normal postage;

(v) Transportation of records or personnel; or

(vi) Producing a copy when the individual has requested only to review the records and has not requested a copy, and the only means of allowing review is to make a copy (e.g., the records are stored in a computer and a copy must be printed to provide individual access, or the activity does not wish to surrender temporarily the original records for the individual to review).

(m) *Privacy Act case files.* (1) Whenever an individual submits a Privacy Act request, a case file will be established. This Privacy Act case file is a specific type of file that is governed by a specific Privacy Act system of records notice. In no instance will the individual's Privacy Act request and corresponding Army actions be included in the individual's military personnel file or other military filing systems, such as adverse action files or general legal files, and in no instance will the Privacy Act case file be used

to make an adverse determination about the individual.

(2) The case file will be comprised of the request for access/amendment, grants, refusals, coordination action(s), and all related papers.

§ 505.6 Amendment of records.

(a) *Amended records.* (1) Individuals are encouraged to periodically review the information maintained about them in Privacy Act systems of records and to familiarize themselves with the amendment procedures established by this part.

(2) An individual may request to amend records that are retrieved by his or her name or personal identifier from a system of records unless the system has been exempted from the amendment provisions of the Act. The standard for amendment is that the records are inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete. The burden of proof is on the requester.

(3) The system manager or custodian must review Privacy Act records for accuracy, relevance, timeliness, and completeness.

(4) Amendment procedures are not intended to permit individuals to challenge events in records that have actually occurred. Amendment procedures only allow individuals to amend those items that are factually inaccurate and not matters of official judgment (e.g., performance ratings, promotion potential, and job performance appraisals). In addition, an individual is not permitted to amend records for events that have been the subject of judicial or quasi-judicial actions/proceedings.

(b) *Proper amendment requests.* (1) Amendment requests, except for routine administrative changes, will be in writing.

(2) When acting on behalf of a first party requester, an individual must provide written documentation of the first party requester's consent to allow the individual to view his or her records.

(3) Amendment is appropriate if it can be shown that—

(i) Circumstances leading up to the recorded event were found to be inaccurately reflected in the document;

(ii) The record is not identical to the individual's copy; or

(iii) The document was not constructed in accordance with the applicable recordkeeping requirements prescribed in AR 25–400–2, The Army Records Information Management System (ARIMS).

(4) Under the amendment provisions, an individual may not challenge the merits of an adverse determination.

(5) U.S. Army Criminal Investigation Command (USACIDC) reports of investigations (PA system of records notice A0195–2a USACIDC, Source Register; A0195–2b USACIDC, Criminal Investigation and Crime Laboratory Files) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195–2. Actions taken by the Commander of U.S. Army Criminal Investigation Command will constitute final action on behalf of the Secretary of the Army under that regulation.

(6) Records placed in the National Archives are exempt from the Privacy Act provision allowing individuals to request amendment of records. Most provisions of the Privacy Act apply only to those systems of records that are under the legal control of the originating agency; for example, an agency's current operating files or records stored at a Federal Records Center.

(7) Inspector General investigative files and action request/complaint files (records in system notice A0021–1 SAIG, Inspector General Records) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 20–1 by the Inspector General. Action by the Inspector General will constitute final action on behalf of the Secretary of the Army under that regulation.

(8) Other records that are exempt from the amendment provisions of the Privacy Act are listed in the applicable PA system of records notices.

(c) *Amendment procedures.* (1) Requests to amend records should be addressed to the custodian or system manager of the records. The request must reasonably describe the records to be amended and the changes sought