

§ 505.6

32 CFR Ch. V (7–1–09 Edition)

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

Department of the Army, DoD

§ 505.6

(e.g., deletion, addition, or amendment). The burden of proof is on the requester. The system manager or records custodian will provide the individual with a written acknowledgment of the request within 10 working days and will make a final response within 30 working days of the date the request was received. The acknowledgment must clearly identify the request and inform the individual that final action will be forthcoming within 30 working days.

(2) Records for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness.

(3) If the amendment is appropriate, the system manager or custodian will physically amend the records accordingly. The requester will be notified of such action.

(4) If the amendment is not warranted, the request and all relevant documents, including reasons for not amending, will be forwarded to the proper Denial Authority within 10 working days to ensure that the 30 day time limit for the final response is met. In addition, the requester will be notified of the referral.

(5) Based on the documentation provided, the Denial Authority will either amend the records and notify the requester and the custodian of the records of all actions taken, or deny the request. If the records are amended, those who have received the records in the past will receive notice of the amendment.

(6) If the Denial Authority determines that the amendment is not warranted, he or she will provide the requester and the custodian of the records reason(s) for not amending. In addition, the Denial Authority will send the requester an explanation regarding his or her right to seek further review by the DA Privacy Act Review Board, through the Denial Authority, and the right to file a concise "Statement of Disagreement" to append to the individual's records.

(1) On receipt of a request for further review by the Privacy Act Review Board, the Denial Authority will append any additional records or background information that substantiates

the refusal or renders the case complete;

(ii) Within 5 working days of receipt, forward the appeal to the DA Privacy Act Review Board; and

(iii) Append the servicing Judge Advocate's legal review, including a determination that the Privacy Act Review Board packet is complete.

(d) *DA Privacy Act Review Board.* (1) The DA Privacy Act Review Board acts on behalf of the Secretary of the Army in deciding appeals of the appropriate Denial Authority's refusal to amend records.

(2) The Board will process an appeal within 30 working days of its receipt. The General Counsel may authorize an additional 30 days when unusual circumstances and good cause so warrant.

(3) The Board membership consists of the following principal members, comprised of three voting and two non-voting members, or their delegates.

(4) Three voting members include—

(i) Administrative Assistant to the Secretary of the Army (AASA) who acts as the Chairman of the Board;

(ii) The Judge Advocate General; and

(iii) The Chief, DA Freedom of Information and Privacy Division, U.S. Army Records Management and Declassification Agency.

(5) In addition, two non-voting members include—

(i) The Chief Attorney, OAASA (or designee) who serves as the legal advisor and will be present at all Board sessions to provide legal advice as required; and

(ii) Recording Secretary provided by the Office of the Administrative Assistant to the Secretary of the Army.

(e) *DA Privacy Act Review Board meetings.* (1) The meeting of the Board requires the presence of all five members or their designated representatives. Other non-voting members with subject matter expertise may participate in a meeting of the Board, at the discretion of the Chairman.

(2) Majority vote of the voting members is required to make a final determination on a request before the Board.

(3) Board members, who have denial authority, may not vote on a matter upon which they took Denial Authority action. However, an individual who

took Denial Authority action, or his or her representative, may serve as a non-voting member when the Board considers matters in the Denial Authority's area of functional specialization.

(4) The Board may seek additional information, including the requester's official personnel file, if relevant and necessary to decide the appeal.

(5) If the Board determines that an amendment is warranted (the record is inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete) it will amend the record and notify the requester, the Denial Authority, the custodian of the record, and any prior recipients of the record, of the amendment.

(6) If the Board determines that amendment is unwarranted, they will—

(i) Obtain the General Counsel's concurrence in writing;

(ii) Respond to the requester with the reasons for denial; and

(iii) Inform the requester of the right to file a "Statement of Disagreement" with the Board's action and to seek judicial review of the Army's refusal to amend. A "Statement of Disagreement" must be received by the system manager within 120 days and it will be made an integral part of the pertinent record. Anyone who may have access to, use of, or need to disclose information from the record will be aware that the record was disputed. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record.

(7) It is inappropriate for the Privacy Act Review Board to consider any record which is exempt from the amendment provision of the Privacy Act.

§ 505.7 Disclosure of personal information to other agencies and third parties.

(a) *Disclosing records to third parties.*

(1) DA is prohibited from disclosing a record from a Privacy Act system of records to any person or agency without the prior written consent of the subject of the record, except when—

(i) Pursuant to the twelve Privacy Act exceptions. The twelve exceptions to the "no disclosure without consent" rule are those exceptions which permit

the release of personal information without the individual's/subject's consent (See appendix C of this part).

(ii) The FOIA requires the release of the record. One of the twelve exceptions to Privacy Act is the FOIA Exception. If the FOIA requires the release of information, the information must be released. The Privacy Act can not prevent release to a third party if the FOIA requires release. However, information must not be discretionarily released under the FOIA if the information is subject to the Privacy Act's "no disclosure without consent" rule.

(iii) A routine use applies. Another major exception to the "no disclosure without consent" rule is the routine use exception. The Privacy Act allows federal agencies to publish routine use exceptions to the Privacy Act. Some routine uses are Army specific, DOD specific, and Governmentwide. Routine uses exceptions are listed in the Privacy Act system of records notice(s) applicable to the Privacy Act records in question. The Army and other agencies' system of records notices may be accessed at the Defense Privacy Office's Web site <http://www.defenselink.mil/privacy>.

(2) The approved twelve exceptions to the Privacy Act "no disclosure without consent" rule are listed at appendix C of this part.

(b) *Disclosing records to other DOD components and to federal agencies outside the DOD.* (1) The twelve Privacy Act exceptions referred to in appendix C of this part are available to other DOD components and to federal agencies outside the DOD as exceptions to the Privacy Act's "no disclosure without consent" rule, with the exception of the FOIA exception. The FOIA is not an appropriate mechanism for providing information to other DOD components and to federal agencies outside the DOD.

(2) A widely used exception to requests for information from local and state government agencies and federal agencies not within the DOD is the routine use exception to the Privacy Act.

(3) The most widely used exception to requests for information from other DOD components is the "intra-agency