

Army Regulation 340-21

Office Management

The Army Privacy Program

**Headquarters
Department of the Army
Washington, DC
5 July 1985**

Unclassified

SUMMARY of CHANGE

AR 340-21

The Army Privacy Program

This revision incorporates only minor administrative changes including updating of office symbols and ZIP codes. A summary of changes made to this regulation will appear on this page in all future issues of this publication. This publication has been reorganized to make it compatible with the Army electronic publishing database. No content has been changed.

Effective 5 July 1985

Office Management

The Army Privacy Program

By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:

DONALD J. DELANDRO
Brigadier General, United States Army
The Adjutant General

History. This UPDATE printing publishes a revision which is effective 5 July 1985. Because the structure of the entire revised text has been reorganized, no attempt has been

made to highlight changes from the earlier regulation dated 27 August 1975.

Summary. This regulation on the Army Privacy Program has been revised. It supplements DOD Directive 5400.11 and DOD 5400.11-R.

Applicability. This regulation applies to the Active Army, the Army National Guard, the U.S. Army Reserve, and the Army and Air Force Exchange Service.

Proponent and exception authority. Not applicable

Army management control process. Supplementation. Supplementation of this regulation is prohibited without prior approval from HQDA(DAAG-AMR-S), ALEX VA 22331-0301.

Interim changes. Interim changes to this

regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of The Adjutant General. Users are invited to send comments and suggested improvements on DA Form 2028(Recommended Changes to Publications and Blank Forms) directly to HQDA(DAAG-AMR-S), ALEX VA 22331-0301.

Distribution. Active Army, B; ARNG, D; USAR, D.

Contents (Listed by paragraph and page number)

Chapter 1

General Information, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Responsibilities • 1-4, page 1

Policy • 1-5, page 1

Authority • 1-6, page 1

Access and amendment refusal authority • 1-7, page 1

DA Privacy Review Board • 1-8, page 2

Privacy official • 1-9, page 2

Chapter 2

Individual Rights of Access and Amendment, page 2

Access under the Privacy Act • 2-1, page 2

Notifying the individual • 2-2, page 2

Relationship between the Privacy Act and the Freedom of Information Act • 2-3, page 2

Functional requests • 2-4, page 2

Medical records • 2-5, page 2

Third party information • 2-6, page 2

Referral of records • 2-7, page 2

Fees • 2-8, page 2

Denial of access • 2-9, page 2

Amendment of records • 2-10, page 3

Procedures • 2-11, page 3

Privacy case files • 2-12, page 3

Chapter 3

Disclosure of Personnel Information to Other Agencies and Third Parties, page 3

Disclosure without consent • 3-1, page 3

Blanket routine use disclosures • 3-2, page 4

Disclosure to third parties • 3-3, page 4

Accounting of disclosure • 3-4, page 4

Chapter 4

Recordkeeping Requirements Under the Privacy Act, page 5

Systems of records • 4-1, page 5

Privacy Act Statement • 4-2, page 5

Social Security Number • 4-3, page 5

Safeguarding personal information • 4-4, page 5

First amendment rights • 4-5, page 5

System notice • 4-6, page 5

Reporting requirements • 4-7, page 6

Rules of conduct • 4-8, page 6

Judicial sanctions • 4-9, page 6

Chapter 5

Exemptions, page 6

Exempting systems of records • 5-1, page 6

General exemptions • 5-2, page 6

Specific exemptions • 5-3, page 6

Procedures • 5-4, page 7

Exempt Army records • 5-5, page 7

Exempt OPM records • 5-6, page 15

Glossary

*This regulation supersedes AR 340-21, 27 August 1975.

RESERVED

Chapter 1 General Information

1-1. Purpose

This regulation sets forth policies and procedures that govern personal information kept by the Department of the Army (DA) in systems of records.

1-2. References

a. Required publications.

(1) AR 195-2, Criminal Investigation Activities. (Cited in para 2-10e.)

(2) AR 340-17, Release of Information and Records from Army Files. (Cited in paras 2-8 and 4-4c.)

(3) AR 340-21-8, The Army Privacy Program; System Notices and Exemption Rules for Civilian Personnel Functions. (Cited in para 2-9c.)

(4) AR 380-380, Automated Systems Security. (Cited in paras 4-4band 4-6c(8).)

b. Related publications. (A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.)

(1) DODD 5400.11, DOD Privacy Program.

(2) DOD 5400.11-R, DOD Privacy Program.

(3) Treasury Fiscal Requirements Manual. This publication can be obtained from The Treasury Department, 15th and Pennsylvania Ave, NW, Washington, DC 20220.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The Assistant Chief of Staff for Information Management (ACSIM) is responsible for issuing policy and guidance for the Army Privacy Program in consultation with the Army General Counsel.

b. The Adjutant General (TAG) is responsible for developing and recommending policy to ACSIM concerning the Army Privacy Program and for overall execution of the program under the policy and guidance of ACSIM.

c. Heads of Army Staff agencies, field operating agencies, major Army commands(MACOMs), and subordinate commands are responsible for supervision and execution of the privacy program in functional areas and activities under their command.

d. Heads of Joint Service agencies or commands for which the Army is the Executive Agent, or otherwise has responsibility for providing fiscal, logistical, or administrative support, will adhere to the policies and procedures in this regulation.

e. Commander, Army and Air Force Exchange Service (AAFES), is responsible for the supervision and execution of the privacy program within that command pursuant to this regulation.

1-5. Policy

Army policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with operational requirements established by the Privacy Act are as follows:

a. Protect, as required by the Privacy Act of 1974 (5 USC 552a), as amended, the privacy of individuals from unwarranted intrusion. Individuals covered by this protection are living citizens of the United States and aliens lawfully admitted for permanent residence.

b. Collect only the personal information about an individual that is legally authorized and necessary to support Army operations. Disclose this information only as authorized by the Privacy Act and this regulation.

c. Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

d. Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

e. Let individuals know what records the Army keeps on them and let them review or get copies of these records, subject to

exemptions authorized by law and approved by the Secretary of the Army. (See chap 5.)

f. Permit individuals to amend records about themselves contained in Army systems of records, which they can prove are factually in error, not up-to-date, not complete, or not relevant.

g. Allow individuals to ask for an administrative review of decisions that deny them access to or the right to amend their records.

h. Maintain only information about an individual that is relevant and necessary for Army purposes required to be accomplished by statute or Executive Order.

i. Act on all requests promptly, accurately, and fairly.

1-6. Authority

The Privacy Act of 1974 (5 USC 552a), as amended, is the statutory basis for the Army Privacy Program. Within the Department of Defense (DOD), the Act is implemented by DODD 5400.11 and DOD 5400-11-R. The Act assigns—

a. Overall Government-wide responsibilities for implementation to the Office of Management and Budget (OMB).

b. Specific responsibilities to the Office of Personnel Management (OPM) and the General Services Administration (GSA).

1-7. Access and amendment refusal authority

Each access and amendment refusal authority (AARA) is responsible for action on requests for access to, or amendment of, records referred to them under this regulation. The officials listed below are the sole AARAs for records in their functional areas:

a. The Adjutant General—for personnel records of Army retired, separated, and reserve military members; DOD dependent school student transcripts; and records not within the jurisdiction of another AARA.

b. The Administrative Assistant to the Secretary of the Army—for records of the Secretariat and its serviced activities, as well as those records requiring the personal attention of the Secretary of the Army.

c. The president or executive secretary of boards, councils, and similar bodies established by DA to consider personnel matters, excluding the Army Board for Correction of Military Records.

d. Chief of Chaplains—for ecclesiastical records.

e. Chief of Engineers—for records pertaining to civil works, including litigation; military construction; engineer procurement; other engineering matters not under the purview of another AARA; ecology; and contractor qualifications.

f. Comptroller of the Army—for financial records.

g. Deputy Chief of Staff for Personnel—for the records listed below.

(1) Personnel records of current Federal civilian employees and active and former nonappropriated fund employees (except those in the AAFES).

(2) Military police records.

(3) Prisoner confinement and correctional records.

(4) Safety records.

(5) Alcohol and drug abuse treatment records.

Note. (Requests from former civilian employees to amend a record in an OPM system of records such as the Official Personnel Folder should be sent to the Office of Personnel Management, Assistant Director for Workforce Information, Compliance and Investigations Group, 1900 E Street, NW, WASH DC 20415-0001.)

h. The Inspector General (TIG)—for TIG investigative records.

i. The Judge Advocate General (TJAG)—for legal records under TJAG responsibility.

j. The Surgeon General—for medical records, except those properly part of the Official Personnel Folder (OPM/GOVT-1 system of records).

k. Commander, AAFES—for records pertaining to employees, patrons, and other matters that are the responsibility of the Exchange Service.

l. Commanding General, U.S. Army Criminal Investigation Command(USACIDC)—for criminal investigation reports and military police reports included therein.

m. Commanding General, U.S. Army Intelligence and Security Command—for intelligence and security investigative records.

n. Commanding General, U.S. Army Materiel Command—for records of Army contractor personnel, exclusive of those in above.

o. Commanding General, U.S. Army Military Personnel Center—for personnel and personnel-related records of Active duty Army members.

p. Commander, Military Traffic Management Command—for transportation records.

q. Chief, National Guard Bureau—for personnel records of the Army National Guard.

1–8. DA Privacy Review Board

The DA Privacy Review Board acts on behalf of the Secretary of the Army to decide appeals from refusal of the appropriate AARAs to amend records. Board membership is comprised of the Administrative Assistant to the Secretary of the Army, The Adjutant General, and The Judge Advocate General, or their representatives. The AARA may serve as a nonvoting member when the Board considers matters in the AARA's area of functional specialization. The Adjutant General chairs the Board and provides the Recording Secretary.

1–9. Privacy official

a. Heads of Army Staff agencies and commanders of MACOMs and subordinate commands and activities will designate a privacy official who will serve as a staff adviser on privacy matters. This function will not be assigned below battalion level.

b. The privacy official will insure that—

- (1) Requests are processed promptly and responsively.
- (2) Records subject to the Privacy Act in his or her command or agency are described properly by a published system notice.
- (3) Privacy statements are included on forms and questionnaires that seek personal information from an individual.
- (4) Procedures are in place to meet reporting requirements.

Chapter 2 Individual Rights of Access and Amendment

2–1. Access under the Privacy Act

a. Upon a written or oral request, an individual, or his or her designated agent or legal guardian, will be granted access to a record pertaining to that individual, maintained in a system of records, unless—

- (1) The record is subject to an exemption and the system manager has invoked the exemption (see chap 5), or
- (2) The record is information compiled in reasonable anticipation of a civil action or proceeding.

b. The requester does not have to state a reason or justify the need to gain access. 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. The request should be submitted to the custodian of the record.

2–2. Notifying the individual

The custodian of the record will acknowledge requests for access within 10 work days of receipt. Releasable records will be provided within 30 days, excluding Saturdays, Sundays, and legal public holidays.

2–3. Relationship between the Privacy Act and the Freedom of Information Act

A Privacy Act request for access to records will be processed also as a Freedom of Information Act request. If all or any portion of the requested material is to be denied, it must be considered under the substantive provisions of both the Privacy Act and the Freedom of Information Act. Any withholding of information must be justified by asserting a legally applicable exemption in each Act.

2–4. Functional requests

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

2–5. Medical records

If it is determined that releasing medical information to the data subject could have an adverse effect on the mental or physical health of that individual, the requester will be asked to name a physician to receive the record. The data subject's failure to designate a physician is not a denial under the Privacy Act and cannot be appealed.

2–6. Third party information

Third party information pertaining to the data subject may not be deleted from a record when the data subject requests access to the record unless there is an established exemption. (See para 5–5.) However, personal data such as SSN and home address of a third party in the data subject's record normally do not pertain to the data subject and therefore may be withheld. Information about the relationship between the data subject and the third party would normally be disclosed as pertaining to the data subject.

2–7. Referral of records

Requests for access to Army systems of records containing records that originated with other DOD components or Federal agencies that claimed exemptions for them will be coordinated with or referred to the originator for release determination. The requester will be notified of the referral.

2–8. Fees

Requesters will be charged only for reproduction of requested documents. Normally, there will be no charge for the first copy of a record provided to an individual to whom the record pertains. Thereafter, fees will be computed as set forth in AR 340–17.

2–9. Denial of access

a. The only officials authorized to deny a request from a data subject for records in a system of records pertaining to that individual are the appropriate AARAs, or the Secretary of the Army, acting through the General Counsel. (See para 1–7.) Denial is appropriate only if the record—

- (1) Was compiled in reasonable anticipation of a civil action or proceeding, or
- (2) Is properly exempted by the Secretary of the Army from the disclosure provisions of the Privacy Act (see chap 5), there is a legitimate governmental purpose for invoking the exemption, and it is not required to be disclosed under the Freedom of Information Act.

b. Requests for records recommended to be denied will be forwarded to the appropriate AARA within 5 workdays of receipt, together with the request, disputed records, and justification for withholding. The requester will be notified of the referral.

c. Within the 30 workday period, the AARA will give the following information to the requester in writing if the decision is to deny the request for access: (See para 2–2.)

- (1) Official's name, position title, and business address.
- (2) Date of the denial.
- (3) Reasons for the denial, including citation of appropriate sections of the Privacy Act and this regulation.

(4) The opportunity for further review of the denial by the General Counsel, Office of the Secretary of the Army, The Pentagon, WASH DC 20310–0104, through the AARA within 60 calendar days. (For denials made by the Army when the record is maintained in one of OPM's Government-wide systems of records, notices for which are described in AR340–21–8, appendix A, an individual's

request for further review must be addressed to the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street, NW, WASH DC 20415-0001.)

2-10. Amendment of records

a. Individuals may request the amendment of their records, in writing, when such records are believed to be inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete.

b. The amendment procedures are not intended to permit challenges of an event in a record that actually occurred, or to permit collateral attack upon an event that has been the subject of a judicial or quasi-judicial action.

c. Consideration of a request for amendment would be appropriate if it can be shown that—

(1) Circumstances leading up to the event recorded on the document were challenged through administrative procedures and found to be inaccurately described.

(2) The document is not identical to the individual's copy, or

(3) The document was not constructed in accordance with the applicable record-keeping requirements prescribed.

d. For an example of above, the amendment provisions do not allow an individual to challenge the merits of an adverse action. However, if the form that documents the adverse action contains an error on the fact of the record (for example, the individual's name is misspelled, or an improper date of birth or SSN was recorded), the amendment procedures may be used to request correction of the record.

e. USACIDC reports of investigation (records in system notices A0501.08e Informant Register, A0508.11b Criminal Information Reports and Cross Index Card Files, and A0508.25a Index to Criminal Investigative Case Files) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195-2 by the Commander, U.S. Army Criminal Investigation Command. Action by the Commander, U.S.-Army Criminal Investigation Command, will constitute final action on behalf of the Secretary of the Army under that regulation.

f. Records placed in the National Archives are exempted 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.

2-11. Procedures

a. Requests to amend a record should be addressed to the custodian or system manager of that record. The request must reasonably describe the record to be amended and the changes sought (that is, deletion, addition, or amendment). The burden of proof rests with the requester; therefore, the alteration of evidence presented to courts, boards, and other official proceedings is not permitted. (An individual acting for the requester must supply a written consent signed by the requester.)

b. The custodian or system manager will acknowledge the request within 10 workdays and make final responses within 30 workdays.

c. The record for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness to assure fairness to the individual in any determination made about that individual on the basis of that record.

d. If the amendment is proper, the custodian or system manager will physically amend the record by adding or deleting information, or destroying the record or a portion of it. He or she will notify the requester of such action.

e. If the amendment is not justified, the request and all relevant documents, including reasons for not amending, will be forwarded to the proper AARA within 5 workdays; the requester will be notified.

f. The AARA, on the basis of the evidence, either will amend the

record and notify the requester and the custodian or deny the request and inform the requester of—

(1) Reasons for not amending.

(2) His or her right to seek further review by the DA Privacy Review Board (through the AARA).

g. On receipt of an appeal from a denial to amend, the AARA will append any additional records or background information that substantiates the refusal or renders the case complete and, within 5 workdays of receipt, forward the appeal to the DA Privacy Review Board.

h. The DA Privacy Review Board, on behalf of the Secretary of the Army, will complete action on a request for further review within 30 workdays of its receipt by the AARA. The General Counsel may authorize an additional 30 days when unusual circumstances and good cause so warrant. The Board may seek additional information, including the appellant's official personnel file, if relevant and necessary to decide the appeal.

(1) If the Board determines that amendment is justified, it will amend the record and notify the requester, the AARA, the custodian of the record, and any prior recipients of the record.

(2) If the Board denies the request, it will obtain the General Counsel's concurrence. Response to the appellant will include reasons for denial and the appellant's right to file a statement of disagreement with the Board's action and to seek judicial review of the Army's refusal to amend.

i. Statements of disagreement will be an integral part of the record to which they pertain so the fact that the record is disputed is apparent to anyone who may have access to, use of, or need to disclose from it. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record. The summary will be limited to the reasons stated to the individual by the Board.

2-12. Privacy case files

Whenever an individual submits a Privacy Act request, a case file will be established. (See system notice A0240.01DAAG.) In no instance will the individual's request and Army actions thereon be included in the individual's personnel file. The case file will comprise the request for access/amendment, grants, refusals, coordination action, and related papers. This file will not be used to make any determinations about the individual.

Chapter 3 Disclosure of Personnel Information to Other Agencies and Third Parties

3-1. Disclosure without consent

The Army is prohibited from disclosing a record from a system of records without obtaining the prior written consent of the data subject, except when disclosure is—

a. Made to officers and employees of DOD who have a need for the record in the performance of their duties.

b. Required under the Freedom of Information Act. (See para 3-3 for information normally releasable.)

c. Permitted by a routine use that has been published in the *Federal Register*.

d. Made to the Bureau of the Census for planning or carrying out a census or survey, or to a related activity pursuant to title 13 of the United States Code.

e. Made to a recipient who has provided the Army with advance written assurance that the record will be—

(1) Used solely as a statistical research or reporting record.

(2) Transferred in a form that is not individually identifiable.

f. Made to the National Archives of the United States as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for determination of such value by the Administrator of the General Services Administration (GSA), or designee. (Records sent to Federal Records Centers for

storage remain under Army control. These transfers are not disclosures and do not therefore need an accounting.)

g. Made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if—

(1) The activity is authorized by law.

(2) The head of the agency or instrumentality has made a written request to the Army element that maintains the record. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.

h. Made to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual. Upon such disclosure notification will be transmitted to the last known address of such individual.

i. Made to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee.

j. Made to the Comptroller General, or authorized representatives, in the course of the performance of the duties of the General Accounting Office(GAO).

k. Pursuant to the order signed by a judge of a court of competent jurisdiction.(Reasonable efforts must be made to notify the subject individual if the legal process is a matter of public record.)

l. Made to a consumer reporting agency under section 3(d) of the Federal Claims Collection Act of 1966 (originally codified at 31 USC 952(d); recodified at 31 USC 3711(f)). The name, address, SSN, and other information identifying the individual; amount, status, and history of the claim; and the agency or program under which the case arose may be disclosed in this instance.

3-2. Blanket routine use disclosures

In addition to routine uses in each system notice, the following blanket routine uses apply to all records from systems of records maintained by the Army except those which state otherwise.

a. *Law enforcement.* Relevant records maintained to carry out Army functions may be referred to Federal, State, local, or foreign law enforcement agencies if the record indicates a violation or potential violation of law. The agency to which the records are referred must be the appropriate agency charged with the responsibility of investigating or prosecuting the violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

b. *Disclosure when requesting information.* A record may be disclosed to a Federal, State, or local agency that maintains civil, criminal, or other relevant enforcement information, or other pertinent information, such as licensing, to obtain data relevant to an Army decision concerning—

(1) Hiring or retention of an employee.

(2) Issuance of a security clearance.

(3) Letting of a contract.

(4) Issuance of a license, grant, or other benefit.

c. *Disclosure of requested information.* If the information is relevant and necessary to the requesting agency's decision, a record may be disclosed to a Federal agency in response to its request in connection with—

(1) Hiring or retention of an employee.

(2) Issuance of a security clearance.

(3) Reporting of an investigation of an employee.

(4) Letting of a contract.

(5) Issuance of a license, grant, or other benefit.

d. *Congressional inquiries.* Disclosure from a system of records maintained by the Army 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.

e. *Private relief legislation.* Relevant information in all systems of records of DOD published on or before August 22, 1975, will be disclosed to OMB for review of private relief legislation, as set forth in OMB Circular A-19. Information may be disclosed at any stage of the legislative coordination and clearance process.

f. *Disclosures required by international agreements.* A record may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities. These disclosures are in compliance with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

g. *Disclosure to State and local taxing authorities.* Any information normally contained in Internal Revenue Service Form W-2, which is maintained in a record from a system of records of the Army, may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 USC 5516, 5517, and 5520; only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use complies with Treasury Fiscal Requirements Manual, sec 5060.

h. *Disclosure to OPM.* A record may be disclosed to OPM concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for OPM to carry out its legally authorized Government-wide personnel management functions and studies.

i. *Disclosure to National Archives and Records Service (NARS), GSA.* A record may be disclosed to NARS, GSA, in records management inspections conducted under 44 USC, 2904 and 2906.

j. *Disclosure to the Department of Justice for litigation.* A record may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing DOD, or any officer, employee, or member of DOD in pending or potential litigation to which the record is pertinent.

3-3. Disclosure to third parties

Personal information that may be disclosed under the Freedom of Information Act is as follows:

a. *Military personnel.*

(1) Name, rank, date of rank, gross salary, present and past duty assignments, future assignments that are officially established, office or duty telephone number, source of commission, promotion sequence number, awards and decorations, military and civilian educational level, and duty status at any given time.

(2) Lists or compilations of unit or office addresses or telephone numbers of military personnel are not released where the requester's primary purpose in seeking the information is to use it for commercial solicitation.

b. *Civilian employees.*

(1) Name and present and past position titles, grades, salaries, and duty stations that include office or duty telephone numbers.

(2) Disclosure of information in (1) above will not be made when the request is a list of present or past position titles, grades, salaries, and/or duty stations and—

(a) Is selected to constitute a clearly unwarranted invasion of personal privacy. For example, the nature of the request calls for a response that would reveal more about the employee than the items in (1) above.

(b) Would be protected from mandatory disclosure under an exemption of the Freedom of Information Act.

(3) In addition to the information in (1) above, the following information may be made available to a prospective employer of a current or former Army employee:

(a) Tenure of employment.

(b) Civil service status.

(c) Length of service in the Army and the Government.

(d) Date and reason for separation shown on SF 50 (Notification of Personnel Action).

3-4. Accounting of disclosure

a. An accounting of disclosure is required whenever a record from an Army system of records is disclosed to someone other than the data subject, except when that record—

(1) Is disclosed to officials within DOD who have a need for it to perform official business.

(2) Is required to be disclosed under the Freedom of Information Act.

b. Since the characteristics of records maintained within the Army vary widely, no uniform method for keeping the disclosure of accounting is prescribed. For most paper records, the accounting may be affixed to the record being disclosed. It must be a written record and consist of—

(1) Description of the record disclosed.

(2) Name, position title, and address of the person to whom disclosure was made.

(3) Date, method, and purpose of the disclosure.

(4) Name and position title of the person making the disclosure.

c. Purpose of the accounting of disclosure is to enable an individual—

(1) To ascertain those persons or agencies that have received information about the individual.

(2) To provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record.

d. When an individual requests such an accounting, the system manager or designee will respond within 10 workdays and inform the individual of the items in *in* above.

e. The only bases for not furnishing the data subject an accounting of disclosures are if disclosure was made for law enforcement purposes under 5 USC 552a(b)(7), or the disclosure was from a system of records for which an exemption from 5 USC 552a(c)(3) has been claimed. (See table 5–1.)

Chapter 4 Recordkeeping Requirements Under the Privacy Act

4–1. Systems of records

a. Notices of all Army systems of records are required by the Privacy Act to be published in the *Federal Register*. An example is at figure 4–1. When new systems are established, or major changes occur in existing systems, which meet the criteria of OMB guidelines summarized in paragraph 4–6b, advance notice must be furnished OMB and the Congress before the system or proposed changes become operational.

b. Uncirculated personal notes, papers, and records that are retained at the author's discretion and over which the Army exercises no control or dominion are not considered Army records within the meaning of the Privacy Act. Individuals who maintain such notes must restrict their use to that of memory aids. Any disclosure from personal notes, either intentional or through carelessness, removes the information from the category of memory aids and the notes then become subject to provisions of the Act.

c. Only personal information that is necessary to accomplish a purpose or mission of the Army, required by Federal statute or Executive Order of the President, will be maintained in Army systems of records. Statutory authority or regulatory authority to establish and maintain a system of records does not convey unlimited authority to collect and maintain all information that may be useful or convenient. The authority is limited to relevant and necessary information.

d. Except for statistical records, most records could be used to determine an individual's rights, benefits, or privileges. To ensure accuracy, personal information to be included in a system of records will be collected directly from the individual if possible. Collection of information from third parties will be limited to verifying information for security or employment suitability or obtaining performance data or opinion-type evaluations.

4–2. Privacy Act Statement

a. Whenever personal information is requested from an individual that will become part of a system of records retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act Statement. This Statement is to ensure that individuals know why this information is

being collected so they can make an informed decision on whether or not to furnish it. As a minimum, the Privacy Act Statement will include the following information in language that is explicit and easily understood and not so lengthy as to deter an individual from reading it:

(1) Cite the specific statute or Executive order, including a brief title or subject, that authorizes the Army to collect the personal information requested. Inform the individual whether or not a response is mandatory or voluntary and any possible consequences of failing to respond.

(2) Cite the principal purposes for which the information will be used.

(3) Cite the probable routine uses for which the information may be used. This may be a summary of information published in the applicable system notice.

b. The above information normally will be printed on the form used to record the information. In certain instances, it may be printed in a public notice in a conspicuous location such as at check-cashing facilities; however, if the individual requests a copy of its contents, it must be provided.

4–3. Social Security Number

Executive Order 9397 authorizes DA to use the SSN as a system to identify Army members and employees. Once a military member or civilian employee of DA has disclosed his or her SSN for purposes of establishing personnel, financial, or medical records upon entry into Army service or employment, the SSN becomes his or her identification number. No other use of this number is authorized. Therefore, whether the SSN alone is requested from the individual, or the SSN together with other personal information, the Privacy Act Statement must make clear that disclosure of the number is voluntary. If the individual refuses to disclose the SSN, the Army activity must be prepared to identify the individual by alternate means.

4–4. Safeguarding personal information

a. The Privacy Act requires establishment of proper administrative, technical, and physical safeguards to—

(1) Ensure the security and confidentiality of records.

(2) Protect against any threats or hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

b. At each location, and for each system of records, an official will be designated to safeguard the information in that system. Consideration must be given to such items as sensitivity of the data need for accuracy and reliability in operations, general security of the area, and cost of safeguards. (See AR 380–380.)

c. Ordinarily, personal information must be afforded at least the protection required for information designated "For Official Use Only." (See AR340–17, chap IV.) Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

4–5. First amendment rights

No record describing how an individual exercises rights guaranteed by the first amendment will be kept unless expressly authorized by Federal statute, by the subject individual, or unless pertinent to and within the scope of an authorized law enforcement activity. Exercise of these rights includes, but is not limited to, religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

4–6. System notice

a. The Army publishes in the *Federal Register* a notice describing each system of records for which it is responsible. A notice contains—

(1) Name and locations of the records.

(2) Categories of individuals on whom records are maintained.

(3) Categories of records in the system.

(4) Authority (statutory or executive order) authorizing the system.

(5) Purpose of the system.

(6) Routine uses of the records, including categories of users and purposes of such uses.

(7) Policies and practices for storing, retrieving, accessing, retaining, and disposing of the records.

(8) Position title and business address of the responsible official.

(9) Procedures an individual must follow to learn if a system of records contains a record about the individual.

(10) Procedures an individual must follow to gain access to a record about that individual in a system of records, to contest contents, and to appeal initial determinations.

(11) Categories of sources of records in the system.

(12) Exemptions from the Privacy Act claimed for the system. (See table 5-1.)

b. New, or altered systems that meet the requirements below require a report to the Congress and OMB. A new system is one for which no system notice is published in the *Federal Register*. An altered system is one that—

(1) Increases or changes the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the system of records.

(2) Expands the types or categories of information maintained.

(3) Alters the manner in which records are organized, indexed, or retrieved to change the nature or scope of those records.

(4) Alters the purposes for which the information is used, or adds a routine use that is not compatible with the purpose for which the system is maintained.

(5) Changes the equipment configuration on which the system is operated, to create potential for either greater or easier access.

c. Report of a new or altered system must be sent to HQDA(DAAG-AMR-S) at least 120 days before the system or changes become operational and include a narrative statement and supporting documentation. The narrative statement must contain the following items:

(1) System identification and name.

(2) Responsible official.

(3) Purpose of the system, or nature of changes proposed (if an altered system).

(4) Authority for the system.

(5) Number (or estimate) of individuals on whom records will be kept.

(6) Information on First Amendment activities.

(7) Measures to assure information accuracy.

(8) Other measures to assure system security. (Automated systems require risk assessment under AR 380-380.)

(9) Relations to State/local government activities. (See fig 4-2.)

d. Supporting documentation consists of system notice for the proposed new or altered system and proposed exemption rule, if applicable.

4-7. Reporting requirements

a. The annual report required by the Privacy Act, as amended by Public Law 97-375, 96 Statute 1821, focuses on two primary areas:

(1) Information describing the exercise of individuals' rights of access to and amendment of records.

(2) Changes or additions to systems of records.

b. Specific reporting requirements will be disseminated each year by HQDA(DAAG-AMR-S) in a letter to reporting elements.

4-8. Rules of conduct

Systems managers will ensure that all personnel, including Government contractors or their employees who are involved in the design, development, operation, maintenance, or control of any system of records are informed of all requirements to protect the privacy of individuals who are subjects of the records.

4-9. Judicial sanctions

The Privacy Act has both civil remedies and criminal penalties for violations of its provisions.

a. Civil remedies An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act.

b. Criminal penalties A member or employee of the Army may be found guilty of a misdemeanor and fined not more than \$5,000 for willfully—

(1) Maintaining a system of records without first meeting the public noticerequirements of publishing in the *Federal Register*.

(2) Disclosing individually identifiable personal information to one not entitled to it.

(3) Asking for or getting another's record under false pretenses.

Chapter 5 Exemptions

5-1. Exempting systems of records

The Secretary of the Army may exempt Army systems of records from certain requirements of the Privacy Act. The two kinds of exemptions are general and specific. The general exemption relieves systems of records from most requirements of the Act; the specific exemptions from only a few. (See table 5-1.)

5-2. General exemptions

Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim the general exemption. To qualify for this exemption, a system must consist of—

a. Information compiled to identify individual criminals and alleged criminals, which consists only of identifying data and arrest records; type and disposition of charges; sentencing, confinement, and release records; and parole and probation status.

b. Information compiled for the purpose of a criminal investigation, including efforts to prevent, reduce, or control crime, and reports of informants and investigators associated with an identifiable individual.

c. Reports identifiable to an individual, compiled at any stage of the process of enforcement of the criminal laws, from arrest or indictment through release from supervision.

5-3. Specific exemptions

The Secretary of the Army has exempted from certain parts of the Privacy Act all properly classified information and a few systems of records that have the following kinds of information. The Privacy Act exemption cited appears in parentheses after each category.

a. Classified information in every Army system of records. This exemption is not limited to the systems listed in paragraph 5-5. Before denying an individual access to classified information, the Access and Amendment Refusal Authority must make sure that it was properly classified under the standards of Executive Order 11652, 12065, or 12356 and that it must remain so in the interest of national defense or foreign policy. (5 USC 552a(k)(1))

b. Investigatory data for law enforcement purposes (other than that claimed under the general exemption). However, if this information has been used to deny someone a right, privilege, or benefit to which the individual is entitled by Federal law, it must be released, unless doing so would reveal the identity of a confidential source. (5 USC 552a(k)(2))

c. Records maintained in connection with providing protective services to the President of the United States or other individuals protected pursuant to 18 USC 3056. (5 USC 552a(k)(3))

d. Statistical data required by statute and used only for statistical purposes and not to make decisions on the rights, benefits, or entitlements of individuals, except for census records that may be disclosed under 13 USC 8. (5 USC 552a(k)(4))

e. Data compiled to determine suitability, eligibility, or qualifications for Federal service, Federal contracts, or access to classified information. This information may be withheld only to the extent

that disclosure would reveal the identity of a confidential source. (5 USC 552a(k)(5))

f. Testing material used to determine if a person is qualified for appointment or promotion in the Federal service. This information may be withheld only if disclosure would compromise the objectivity or fairness of the examination process. (5 USC 552a(k)(6))

g. Information to determine promotion potential in the Armed Forces. Information may be withheld, but only to the extent that disclosure would reveal the identity of a confidential source. (5 USC 552a(k)(7))

5-4. Procedures

a. When a system manager seeks an exemption for a system of records, the following information will be furnished to HQDA(DAAG-AMR-S), Alexandria, VA 22331-0301:

- (1) Applicable system notice.
- (2) Exemptions sought.
- (3) Justification.

b. After appropriate staffing and approval by the Secretary of the Army, a proposed rule will be published in the *Federal Register*, followed by a final rule 30 days later. No exemption may be invoked until these steps have been completed.

5-5. Exempt Army records

The following records are exempt from certain parts of the Privacy Act:

a. ID-AO224.04DAIG.

(1) *Sysname*. Inspector General Investigative Files.

(2) *Exemption*. All portions of this system of records that fall within 5 USC 552a(k)(2) or (5) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(k)(2) and (5).

(4) *Reasons*. Selected portions and/or records in this system are compiled for the purposes of enforcing civil, criminal, or military law, including Executive orders or regulations validly adopted pursuant to law. Granting individuals access to information collected and maintained in these files could interfere with enforcement proceedings; deprive a person of a right to fair trial or an impartial adjudication or be prejudicial to the conduct of administrative action affecting rights, benefits, or privileges of individuals; constitute an unwarranted invasion of personal privacy; disclose the identity of a confidential source; disclose nonroutine investigative techniques and procedures, or endanger the life or physical safety of law enforcement personnel; violate statutes which authorize or require certain information to be withheld from the public such as: trade or financial information, technical data, National Security Agency information, or information relating to inventions. Exemption from access necessarily includes exemption from the other requirements.

b. ID-AO224.05DAIG.

(1) *Sysname*. Inspector General Action Request/Complaint Files.

(2) *Exemption*. All portions of this system of records which fall within 5 USC 552a(k)(2) or (5) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(k)(2) and (5).

(4) *Reasons*. Selected portions and/or records in this system are compiled for the purposes of enforcing civil, criminal, or military law, including executive orders or regulations validly adopted pursuant to law. Granting individuals access to information collected and maintained in these files could interfere with enforcement proceedings; deprive a person of a right to fair trial or an impartial adjudication or be prejudicial to the conduct of administrative action affecting rights, benefits, or privileges of individuals; constitute an unwarranted invasion of personal privacy; disclose the identity of a confidential source; disclose nonroutine investigative techniques and procedures, or endanger the life or physical safety of law enforcement personnel; violate statutes that authorize or require certain information to be withheld from the public such as trade or financial information, technical data, National Security Agency information, or information relating to inventions. Exemption from access necessarily includes exemption from the other requirements.

c. ID-AO239.01DAAG.

(1) *Sysname*. Request for Information Files.

(2) *Exemption*. Portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g). Portions of the system maintained by offices of Initial Denying Authorities that do not have a law enforcement mission and that fall within 5 USC 552a(k)(1) through (k)(7) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(j)(2) and (k)(1) through (k)(7).

(4) *Reasons*. This system of records is maintained solely for the purpose of administering the Freedom of Information Act and processing routine requests for information. To ensure an accurate and complete file on each case, it is sometimes necessary to include copies of records that have been the subject of a Freedom of Information Act request. This situation applies principally to cases in which an individual has been denied access and/or amendment of personal records under an exemption authorized by 5 USC 552. The same justification for the original denial would apply to a denial of access to copies maintained in the Freedom of Information Act file. It should be emphasized that the majority of records in this system are available on request to the individual and that all records are used solely to process requests. This file is not used to make any other determinations on the rights, benefits, or privileges of individuals.

d. ID-AO240.01DAAG.

(1) *Sysname*. Privacy Act Case Files.

(2) *Exemptions*. Portions of this system that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g). Portions of this system maintained by the DA Privacy Review Board and by those Access and Amendment Refusal Authorities that do not have a law enforcement mission and that fall within 5 USC 552a(k)(1) through (k)(7) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(j)(2) and (k)(1) through (k)(7).

(4) *Reasons*. This system of records is maintained solely for the purpose of administering the Privacy Act of 1974. To ensure an accurate and complete file on each case, it is sometimes necessary to include copies of records which have been the subject of a Privacy Act request. This situation applies principally to cases in which an individual has been denied access and/or amendment of personnel records under an exemption authorized by 5 USC 552a. The same justification for the original denial would apply to a denial of access and/or amendment of copies maintained in the Privacy Act Case File. It should be emphasized that the majority of records in this system are available on request to the individual and that all records are used solely to administer Privacy Act requests. This file is not used to make any other determinations on the rights, benefits, or privileges of individuals.

e. ID-AO241.01HQDA.

(1) *Sysname*. HQDA Correspondence and Control/Central File System.

(2) *Exemption*. Portions of this system of records that fall within 5 USC 552a(k)(1) through (k)(7) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(k)(1) through (k)(7).

(4) *Reasons*. Documents are generated by other elements of the Army or are received from other agencies and individuals. Because of the broad scope of the contents of this system and since the introduction of documents is largely unregulatable, specific portions or documents that may require an exemption cannot be predetermined. Therefore, and to the extent that such material is received and maintained, selected individual documents may be exempted from disclosure under any of the provisions of 5 USC 552a(k)(1) through (k)(7).

f. ID-AO401.08DAJA.

(1) *Sysname*. Prosecutorial Files.

(2) *Exemption.* Portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (e)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence; the identification of offenders or alleged offenders; nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from other requirements.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

g. *ID-AO402.01aDAJA.*

(1) *Sysname.* General Legal Files.

(2) *Exemption.* Those portions of this system of records falling within 5 USC 552a(k)(1), (2), (5), (6), and (7) may be exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), (5), (6), and (7).

(4) *Reasons.* Various records from other exempted systems of records are sometimes submitted for legal review or other action. A copy of such records may be permanently incorporated into the General Legal Files system of records as evidence of the facts upon which a legal opinion or review was based. Exemption of the General Legal Files system of records is necessary in order to ensure that such records continue to receive the same protection afforded them by exemptions granted to the system of records in which they were originally filed

h. *ID-AO404.02DAJA.*

(1) *Sysname.* Courts-Martial Files.

(2) *Exemption.* All portions of this system that fall under 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (d)(2), (d)(3), (d)(4), (e)(2), (e)(3), (e)(4)(H), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.* Courts-martial files are exempt because a large body of existing criminal law governs trials by court-martial to the exclusion of the Privacy Act. The Congress recognized the judicial nature of court-martial proceedings and exempted them from the Administrative Procedures Act by specifically excluding them from the definition of the term "agency" (5 USC 551(1)(f)). Substantive and procedural law applicable in trials by court-martial is set forth in the Constitution, the Uniform Code of Military Justice (UCMJ) Manual for Courts-Martial, 1984, and the decisions of the U.S. Court of

Military Appeals and Courts of Military Review. The right of the accused not to be compelled to be a witness against himself or herself and the need to obtain accurate and reliable information with regard to criminal misconduct necessitate the collection of information from sources other than the individual accused.

(a) Advising the accused or any other witness of the authority for collection of the information, the purpose for which it is to be used, whether disclosure is voluntary or mandatory, and the effects on the individual of not providing the information would unnecessarily disrupt and confuse court-martial proceedings. It is the responsibility of the investigating officer or military judge to determine what information will be considered as evidence. In making the determination, the individual's rights are weighed against the accused's right to a fair trial. The determination is final for the moment and the witness' failure to comply with the decision would delay the proceeding and may result in prosecution of the witness for wrongful refusal to testify.

(b) In a trial by court-martial, the accused has a unique opportunity to assure that the record is accurate, relevant, timely, and complete as it is made. He or she has the right to be present at the trial, to be represented by counsel at general and special courts-martial, and to consult with counsel in summary courts-martial, to review and challenge all information before it is introduced into evidence, to cross-examine all witnesses against him or her, to present evidence in his or her behalf, and in general and special courts-martial, to review and comment upon the record of trial before it is authenticated. Procedures for correction of the record are controlled by the Manual for Courts-Martial, 1984. After completion of appellate review, the record may not be amended. The Uniform Code of Military Justice (10 USC 876) provides that the proceedings, findings, and sentences of courts-martial as approved, reviewed, or affirmed are final and conclusive and binding upon all departments, courts, agencies, and officers of the United States subject only to action upon a petition for new trial, action by the Secretary concerned, and the authority of the President.

i. *ID-AO501.08eUSACIDC.*

(1) *Sysname.* Informant Register.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(3) because release of accounting of disclosures would provide the informant with significant information concerning the nature of a particular investigation, the internal methods and techniques involved in criminal investigation, and the investigative agencies (State, local or foreign) involved in a particular case resulting in a serious compromise of the criminal law enforcement processes.

(b) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because disclosure of portions of the information in this system of records would seriously impair the prudent and efficient handling of these uniquely functioning individuals; hamper the inclusion of comments and evaluations concerning the performance qualification, character, identity, and propensities of the informant; and prematurely compromise criminal investigations which either concern the conduct of the informant, or investigations wherein he or she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records and civil liability predicated upon agency compliance with specific provisions of the Privacy Act.

(c) From subsections (d), (e)(4)(G), (e)(4)(H), and (f) are also necessary to protect the security of information properly classified in the interest of national defense and foreign policy.

(d) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing what information concerning informants is relevant or necessary. Due to close liaison and existing relationships with other Federal, State,

local, and foreign law enforcement agencies, information about informants may be received, which may relate to a case then under the investigative jurisdiction of another Government agency; but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of both the USACIDC and other agencies. Additionally, the failure to maintain all known information about informants could affect the effective utilization of the individual and substantially increase the operational hazards incumbent in the employment of an informant in very compromising and sensitive situations.

(e) From subsection (e)(2) because collecting information from the informant would potentially thwart both the criminal investigative process and the required management control over these individuals by appraising the informant of investigations or management actions concerning his or her involvement in criminal activity or with USACIDC personnel.

(f) From subsection (e)(3) because supplying an informant with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the cooperation of the informant, and render ineffectual investigative techniques and methods utilized by USACIDC in the performance of its criminal law enforcement duties.

(g) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due to type of records maintained and necessity for rapid information retrieval and dissemination. Also, in the collection of information about informants, it is impossible to determine what information is then accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation or contact brings new details to light. In the criminal investigative process, accuracy and relevance of information concerning informants can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting information relating to informant's actions and would impede the development of criminal intelligence necessary for effective law enforcement.

(h) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

j. ID-AO501.10DAMI.

(1) *Sysname.* Counterintelligence Research File System(CIRFS).

(2) *Exemption.* All portions of this system of records which fall within 5 USC 552a(k)(1), (2), or(5) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G),(e)(4)(H), (e)(4)(I), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Information in the files is obtained from overt and sensitive intelligence sources, and contains information classified in the interest of national security under the provisions of EO 12356 and predecessor orders. The system contains investigatory material compiled for law enforcement purposes as well as for determining the suitability for employment or military service and thus will also require the protection of confidential sources. Information may reflect the efforts of hostile intelligence services in the collection effort against the U.S. Army. Additionally, the following factors are at issue in disclosure of data from this system of records: release of exempted information would endanger the safety of sources involved in intelligence programs; release would invade the privacy of those individuals involved in intelligence programs; release would compromise and thus negate specialized techniques used to support intelligence programs; and release would interfere with and negate the orderly conduct of intelligence operations. Exemption from the remaining provisions is predicated upon the exemption from disclosure or upon the need for conducting complete and proper investigations.

k. ID-AO502.03DAMI.

(1) *Sysname.* Intelligence Collection Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(1), (2) or (5)are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Executive Order 12356 and predecessor orders provide for the protection of some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our Allies. To protect against actions hostile to the United States, of both overt and covert nature, it is essential that such official information and material be given only limited dissemination. This exemption is also essential to protect the privacy and personal safety of the sources involved. It is vital to the conduct of secure operations under Director, Central Intelligence Directives 4 and 5 and Defense Intelligence Agency Manual 58-11. Additionally, the disclosure of data within this system of records is exempt to the extent the disclosure of such data would reveal the identity of sources who furnished information to the Government under an express or implied promise that source identities would be held in confidence. These assurances are essential to the candid disclosure of information that is essential to the investigative purpose. Confidence in the integrity of government assurances must be maintained or the investigative process will be severely damaged. Exemption from the other requirements is premised on and follows from the rationale that requires exemption from access.

l. ID-AO502.03bDAMI.

(1) *Sysname.* Technical Surveillance Index.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(1), (2), or (5)are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I).

(3) *Authority.* 5 USC 552a(k)(1), (2), or (5).

(4) *Reasons.* The material contained in this record system contains data concerning sensitive sources and operational methods whose dissemination must be strictly controlled because of national security intelligence considerations. Disclosure of documents or the disclosure accounting record may compromise the effectiveness of the operation, and negate specialized techniques used to support intelligence or criminal investigative programs, or otherwise interfere with the orderly conduct of intelligence operations or criminal investigations.

m. ID-AO502.10aDAMI.

(1) *Sysname.* USAINTA Investigative File System.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(1), (2), or (5)are exempt from the following provisions of 5 USC 552a: (d), (e)(4)(G), (e)(4)(H), and(e)(4)(I).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Executive Order 12356 and predecessor orders provides for the protection of some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our Allies. To protect against actions hostile to the United States, of both overt and covert nature, it is essential that such official information and material be given only limited dissemination. Additionally, in the conduct of such operations which produce these records, at times the methods and arrangements with our Allies pertinent to the conduct of intelligence operations are relevant to this issue of national security interests and must be safeguarded. Further, the disclosure of unclassified data within this record system is exempt only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express or implied promise that the identity of the source would be held in confidence. These assurances are essential to the candid disclosure of information that is essential to the purposes of these investigations. Confidence in the integrity of the Government's assurances must be maintained or the investigative process will be severely damaged. Exemption from the other

requirements is premised on and follows from the rationale that requires exemption from access.

n. ID-AO503.03aDAMI.

(1) *Sysname.* Department of the Army Operational Support Activities Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(1), (2), or (5) are exempt from the following provisions of 5 USC 552a: (c)(3), (d), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Executive Order 12356 and predecessor orders provide for the protection of official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be limited in its accessibility. To protect against hostile actions, both overt and covert, it is essential that such official information and material be given only limited dissemination. Additionally, the following factors are at issue in disclosure of data from this system of records: release of exempted information would endanger the safety of sources involved in intelligence programs; release would invade the privacy of those individuals involved in intelligence programs; release would compromise and thus negate specialized techniques used to support intelligence programs; and release would interfere with and negate the orderly conduct of intelligence operations. Exemption from the other provisions is premised on and follows from the rationale that exempts access to this system of records.

o. ID-AO503.06aDAMI.

(1) *Sysname.* Counterintelligence Operations File.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(1), (2) or (5) are exempt from provisions of 5 USC 552a: (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Executive Order 12356 and predecessor orders provide for the protection of official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be limited in its accessibility. To protect against hostile actions, both overt and covert, it is essential that such official information and material be given only limited dissemination. Additionally, the following factors are at issue in disclosure of data from this system of records: release of exempted information would endanger the safety of sources involved in intelligence programs; release would invade the privacy of those individuals involved in intelligence programs; release would compromise and thus negate specialized techniques used in support of intelligence programs; and release would interfere with and negate the orderly conduct of intelligence operations. Relevant to the above considerations, exemption is necessary from the requirements to provide an individual an accounting of disclosures and to inform an individual whether a record exists on him or her within this system of records, during the period in which an investigative interest and activity remains concerning that individual. Exemption is necessary to avoid disclosure of the existence of ongoing law enforcement investigations and compromise of the purposes and objectives for such ongoing investigations. Further, the disclosure of data within this record system is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express or implied promise that the identity of the source would be held in confidence. These assurances are essential to the candid disclosure of information, which is essential to the purposes of these investigations. Confidence in the integrity of the Government's assurances must be maintained or the investigative process will be severely damaged. The exemption of an individual's right of access to records on him or her in this system of records and the reasons therefor necessitate and provide the rationale for the exemption of this system of records from the requirements of amendment and other cited provisions. Maintaining information that is strictly relevant to law enforcement purposes may result in exclusion of seemingly irrelevant data of significant value in determining the qualifications and suitability of

individuals for Federal civilian employment, military service, Federal contracts, or access to classified information.

p. ID-AO506.01fDAMI.

(1) *Sysname.* Personnel Security Clearance Information Files.

(2) *Exemption.* All portions of this system which fall within 5 USC 552a(k)(1), (2), or (5) are exempt from the following provisions of 5 USC 552a: (d), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

(3) *Authority.* 5 USC 552a(k)(1), (2), and (5).

(4) *Reasons.* Material contained in this record system that is properly and currently classified under Executive Order 12356 and predecessor orders includes data concerning sensitive source and operational methods whose dissemination must be strictly controlled because of its relationship to national security intelligence considerations. Additionally, in the conduct of operations that produce these records, at times the methods and arrangements with our Allies pertinent to the conduct of intelligence operations are relevant to this issue of national security interests and must be safeguarded. Further, the disclosure of unclassified data is exempt only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of 5 USC 552a, under an implied promise that the identity of the source would be held in confidence. These assurances are essential to the purposes of these investigations. Confidence in the integrity of the Government's assurance must be maintained or the investigative process will be severely damaged. Exemption from access necessarily includes exemption from the other requirements.

q. ID-AO508.07USACIDC.

(1) *Sysname.* Criminal Investigation Accreditation Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(2), (5), or (7) are exempt from the following provisions of 5 USC 552a: (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority.* 5 USC 552a(k)(2), (5), and (7).

(4) *Reasons.*

(a) From subsections (d), (e)(4)(G), (e)(4)(H), and (f) because disclosure of portions of the information in this system of records would seriously impair the selection and management of these uniquely functioning individuals; hamper the inclusion of comments, reports, and evaluations concerning the performance, qualifications, character, actions, and propensities of the agent; and prematurely compromise investigations which either concern the conduct of the agent himself or herself or investigations wherein he or she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemptions from the amendment and the agency procedures that would otherwise be required to process these types of requests.

(b) From subsection (e)(1) because the failure to maintain all known information about agents could affect the effective utilization of the individual and substantially increase the operational hazards incumbent in the employment of agents in very compromising and sensitive situations.

r. ID-AO508.11aUSACIDC.

(1) *Sysname.* Criminal Investigation and Crime Laboratory Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning coordinated investigative effort and techniques and the nature of the investigation, resulting in a serious impediment to criminal law enforcement activities or the compromise of properly classified material.

(b) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because access might compromise ongoing investigations, reveal classified information, investigatory techniques or the identity of

confidential informants, or invade the privacy of persons who provide information in connection with a particular investigation. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil liability predicated upon agency compliance with those specific provisions of the Privacy Act. The exemption from access necessarily includes exemption from other requirements.

(c) From subsection (e)(1) because the nature of the investigative function creates unique problems in prescribed specific perimeters in a particular case as to what information is relevant or necessary. Also, due to close liaison and working relationships with other Federal, State, local, and foreign law enforcement agencies, information may be received that may relate to a case then under the investigative jurisdiction of another Government agency, but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of both the USACIDC and other agencies.

(d) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigative process by placing the subject of the investigation on notice thereof.

(e) From subsection (e)(3) because supplying an individual with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the cooperation of the individual queried, and render ineffectual investigation techniques and methods utilized by the USACIDC in the performance of their criminal law enforcement duties.

(f) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due to the great volume of records maintained and the necessity for rapid information retrieval and dissemination. Also, in the collection of information for law enforcement purposes, it is impossible to determine what information is then accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. In the criminal investigative process, accuracy and relevance of information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(g) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

s. ID-AO508.11bUSACIDC.

(1) *Sysname.* Criminal Information Reports and Cross Index Card Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(3) *Authority.* 5 USC a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning coordinated investigative effort and techniques and the nature of the investigation, resulting in a serious impediment to criminal law enforcement activities or the compromise of properly classified material.

(b) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because access might compromise ongoing investigations, reveal investigatory techniques and the identity of confidential informants, and invade the privacy of persons who provide information in connection with a particular investigation. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil

liability predicated upon agency compliance with those specific provisions of the Privacy Act. In addition, subsections (d), (e)(4)(G), (e)(4)(H), and (f) are necessary to protect the security of information properly classified in the interest of national and foreign policy.

(c) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing specific perimeters in a particular case what information is relevant or necessary. Also, due to close liaison and working relationships with other Federal, State, local, and foreign law enforcement agencies, information may be received that may relate to a case then under the investigative jurisdiction of another Government agency, but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of both the USACIDC and other agencies.

(d) From subsection (e)(2) because collecting information from the subject of criminal investigation would thwart the investigative process by placing the subject of the investigation on notice thereof.

(e) From subsection (e)(3) because supplying an individual with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the cooperation of the individuals queried, and render ineffectual investigative techniques and methods utilized by USACIDC in the performance of their criminal law enforcement duties.

(f) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due to the great volume of records maintained and the necessity for rapid information retrieval and dissemination. Also, in the collection of information for law enforcement purposes, it is impossible to determine what information is then accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. In the criminal investigative process, accuracy and relevance of information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(g) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

t. ID-AO508.16DAPE

(1) *Sysname.* Absentee Case Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration, or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law

enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

u. ID-AO508.24aDAPE.

(1) *Sysname.* Serious Incident Reporting Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

v. ID-AO508.25aUSACIDC.

(1) *Sysname.* Index to Criminal Investigative Case Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning coordinated investigative effort and techniques and the nature of the investigation, resulting in a serious impediment to criminal law enforcement activities or the compromise of properly classified material.

(b) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because access might compromise ongoing investigations, reveal investigatory techniques and the identity of confidential informants, and invade the privacy of persons who provide information in connection with a particular investigation. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil liability predicated upon agency compliance with those specific provisions of the Privacy Act. In addition, subsections (d), (e)(4)(G), (e)(4)(H), and (f) are necessary to protect the security of information properly classified in the interest of national and foreign policy.

(c) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing specific perimeters in a particular case what information is relevant or necessary. Also, due to close liaison and working relationships with other Federal, State, local and foreign law enforcement agencies, information may be received that may relate to a case then under the investigative jurisdiction of another Government agency, but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity that may relate to the jurisdiction of both the USACIDC and other agencies.

(d) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigative process by placing the subject of the investigation on notice thereof.

(e) From subsection (e)(3) because supplying an individual with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the cooperation of the individuals queried, and render ineffectual investigative techniques and methods utilized by USACIDC in the performance of their criminal law enforcement duties.

(f) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due to the great volume of records maintained and the necessity for rapid information retrieval and dissemination. Also, in the collection of information for law enforcement purposes, it is impossible to determine what information is then accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. In the criminal investigative process, accuracy and relevance of information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(g) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

w. ID-AO509.08DAPE.

(1) *Sysname.* Registration and Permit Files.

(2) *Exemption.* This system of records insofar as it contains information falling within 5 USC 552a(k)(2) is exempted from the following provisions of 5 USC 552a:(c)(3).

(3) *Authority.* 5 USC 552a(k)(2).

(4) *Reasons.* From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation thus resulting in a serious impediment to criminal law enforcement investigations, activities, or the compromise of properly classified material.

x. ID-AO509.10DAPE.

(1) *Sysname.* Law Enforcement: Offense Reporting System(MPMIS).

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration, or destruction of evidence; the identification of offenders or alleged offenders; nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses, and their families and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual, investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it would compromise the existence of a confidential investigation, or reveal the identity of witnesses or confidential informants.

(e) From section (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

y. *ID-AO509.18bDAPE*.

(1) *Sysname*. Expelled or Barred Person Files.

(2) *Exemption*. All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority*. 5 USC 552a(j)(2).

(4) *Reasons*.

(a) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, and the nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses, and their families and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation.

(b) From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

z. *ID-AO509.19DAPE*.

(1) *Sysname*. Military Police Investigator Certification Files.

(2) *Exemption*. All portions of this system of records that fall within 5 USC 552a(k)(2), (5), or (7) are exempt from the following provisions of 5 USC 552a: (d), (e)(4)(G), (e)(4)(H), and (f).

(3) *Authority*. 5 USC 552a(k)(2), (5), and (7).

(4) *Reasons*. From subsections (d), (e)(4)(G), (e)(4)(H), and (f) because disclosure of portions of the information in this system of records would seriously impair the selection and management of these uniquely functioning individuals; hamper the inclusion of comments, reports and evaluations concerning the performance, qualifications, character, actions, and propensities of the agent; and prematurely compromise investigations which either concern the conduct of the agent himself or herself, or investigations wherein he or she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemptions from the amendment and the agency procedures that would otherwise be required to process these types of requests.

aa. *ID-AO509.21DAPE*.

(1) *Sysname*. Local Criminal Information Files.

(2) *Exemptions*. All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority*. 5 USC 552a(j)(2).

(4) *Reasons*.

(a) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration, or destruction of evidence; the identification of offenders or alleged offenders; nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses, and their families and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because, in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

ab. *ID-AO511.05DAPE*.

(1) *Sysname*. Traffic Law Enforcement/Vehicle Registration System:MPMIS.

(2) *Exemption*. All portions of this system of records that fall within 5 USC 552a(j)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(3) *Authority*. 5 USC 552a(j)(2).

(4) *Reasons.*

(a) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration, or destruction of evidence; the identification of offenders or alleged offenders; nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses, and their families and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(b) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(c) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(d) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(e) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures, or evidence.

ac. ID-AO702.03aUSAREC.

(1) *Sysname.* Enlistment Eligibility Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(5) are exempt from the following provisions of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a(k)(5).

(4) *Reasons.* It is imperative that the confidential nature of evaluations and investigatory material on applicants applying for enlistment furnished to the U.S. Army Recruiting Command under an express promise of confidentiality be maintained to ensure the candid presentation of information necessary in determinations of enlistment and suitability for enlistment into the United States Army.

ad. ID-AO702.08aDASG.

(1) *Sysname.* Army Medical Procurement Applicant Files.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(5) are exempt from the following provisions of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a (k)(5).

(4) *Reasons.* It is imperative that the confidential nature of evaluation and investigatory material on applicants furnished to the Army Medical Procurement Program under an express promise of confidentiality be maintained to ensure that candid presentation of information necessary in determinations involving selection for AMEDD training programs and for suitability for commissioned service and future promotion.

ae. ID-AO704.10bMEPCOM.

(1) *Sysname.* ASVAB Institutional Test Scoring and Reporting System.

(2) *Exemption.* All portions of this system that fall within 5 USC 552a(k)(6) are exempt from the following provision of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a(k)(6).

(4) *Reasons.* Exemption is needed for the portion of records that pertains to individual item response on tests, to preclude compromise of scoring keys.

af. ID-AO709.01aDAPE.

(1) *Sysname.* United States Military Academy Candidate Files.

(2) *Exemption.* All portions of this system that fall within 5 USC 552a(k)(5), (6), or (7) are exempt from the following provisions of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a(k)(5), (6), and (7).

(4) *Reasons.*

(a) From subsection (d) because access might reveal investigatory and testing techniques. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil liability predicated upon agency compliance with those specific provisions of the Privacy Act.

(b) Exemption is necessary to protect the identity of individuals who furnished information to the U.S. Military Academy, which is used in determining suitability, eligibility, or qualifications for military service and which was provided under an express promise of confidentiality.

(c) Exemption is needed for the portion of records compiled within the Academy that pertain to testing or examination material used to rate individual qualifications, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.

(d) Exemption is required for evaluation material used by the Academy in determining potential for promotion in the Armed Services, to protect the identity of a source who furnished information to the Academy under an express promise of confidentiality.

ag. ID-AO709.03DAPE.

(1) *Sysname.* U.S. Military Academy Personnel Cadet Records.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(k)(5) or (7) are exempt from the following provisions of 5 USC 552a: (d)

(3) *Authority.* 5 USC 552a(k)(5) and (7).

(4) *Reasons.* It is imperative that the confidential nature of evaluation and investigatory material on candidates, cadets, and graduates, furnished to the U.S. Military Academy under promise of confidentiality be maintained to ensure the candid presentation of information necessary in determinations involving admission to the Military Academy and suitability for commissioned service and future promotion.

ah. ID-AO713.09aTRADOC.

(1) *Sysname.* Skill Qualification Test.

(2) *Exemption.* All portions of this system that fall under 5 USC 552a(k)(6) are exempt from the following provision of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a(K)(6).

(4) *Reasons.* An exemption is required for those portions of the Skill Qualification Test system pertaining to individual item responses and scoring keys to preclude compromise of the test and to ensure fairness and objectivity of the evaluation system.

ai. ID-AO720.04DAPE.

(1) *Sysname.* Army Correctional System: Correctional Treatment Records.

(2) *Exemption.* All portions of this system of records that fall within 5 USC 552a(J)(2) are exempt from the following provisions of 5 USC 552a: (c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(3) *Authority.* 5 USC 552a(j)(2).

(4) *Reasons.* Granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with the orderly administration of justice. Disclosure of this information could jeopardize the safety and well-being of information sources, correctional supervisors, and other confinement facility administrators. Disclosure of the information could also result in the invasion of privacy of persons who provide information used in developing individual treatment programs. Further, disclosure could result in a deterioration of a prisoner's self-image and adversely affect meaningful relationships between a prisoner and his or her counselor or supervisor. These factors are, of course, essential to the rehabilitative process. Exemption from the remaining provisions is predicated upon the exemption

from disclosure, or upon the need for proper functioning of correctional programs.

aj. ID-AO917.10DASG.

(1) *Sysname.* Family Advocacy Case Management Files.

(2) *Exemption.* All portions of this system that fall within 5 USC 552a (k)(2) and (5) are exempt from the following provision of 5 USC 552a: (d).

(3) *Authority.* 5 USC 552a(k)(2) and (5).

(4) *Reasons.* Exemptions are needed in order to encourage persons having knowledge of abusive or neglectful acts toward children to report such information and to protect such sources from embarrassment or recriminations as well as to protect their right to privacy. It is essential that the identities of all individuals who furnish information under an express promise of confidentiality be protected. In the case of spouse abuse, it is important to protect the privacy of spouses seeking treatment. Additionally, granting individuals access to information relating to criminal and civil law enforcement could interfere with ongoing investigations and the orderly administration of justice in that it could result in the concealment, alteration, destruction, or fabrication of information; could hamper the identification of offenders or alleged offenders; and the disposition of charges; and could jeopardize the safety and well-being of parents, children, and abused spouses.

ak. ID-A1012.01DPE.

(1) *Sysname.* Applicants/Students, US Military Academy Prep School.

(2) *Exemption.* Parts of this system that fall within 5 USC 552a(k)(5) and (7) are exempt from subsection (d) of 5 USC 552a.

(3) *Authority.* 5 USC 552a(k)(5) and (7).

(4) *Reasons.* It is imperative that the confidential nature of evaluation material on individuals, furnished to the U.S. Military Academy Preparatory School under an express promise of confidentiality, be maintained to ensure the candid presentation of information necessary in determinations involving admission to or retention at the U.S. Military Academy Preparatory School and subsequent admission to the U.S. Military Academy and suitability for commissioned military service.

5-6. Exempt OPM records

Three OPM systems of records apply to Army employees, except for nonappropriated fund employees. These systems, the specific exemptions determined to be necessary and proper, the records exempted, provisions of the Privacy Act from which exempted, and justification are set forth below.

a. Personnel Investigations Records (OPM/CENTRAL-9).

(1) All material and information in these records that meets the criteria stated in 5 USC 552a(k)(1), (2), (3), (5), and (6) is exempt from the requirements of 5 USC 552a(c)(3) and (d). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject and access to and amendment of records.

(2) The specific applicability of the exemptions to this system and the reasons for the exemptions are as follows:

(a) Personnel investigations may obtain from another Federal agency, properly classified information that pertains to National defense and foreign policy. Application of exemption(k)(1) may be necessary to preclude the data subject's access to and amendment of such classified information under 5 USC 552a(d).

(b) Personnel investigations may contain investigatory material compiled for law enforcement purposes other than material within the scope of 5 USC 552a(j)(2), e.g., investigations into the administration of the merit system. Application of exemption (k)(2) may be necessary to preclude the data subject's access to or amendment of such records, under 552a(c)(3) and (d).

(c) Personnel investigations may obtain from another Federal agency information that relates to providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18. Application of exemption (k)(3) may be necessary to preclude the data subject's access to and amendment of such records under 5 USC 552a(d).

(d) All information about individuals in these records that meets the criteria stated in 5 USC 552a(k)(5) is exempt from the requirements of 5 USC 552a(c)(3) and (4). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject and access to and amendment of records.

(e) All material and information in these records that meets the criteria stated in 5 USC 552a(k)(6) is exempt from the requirements of 5 USC 552a(d), relating to access to and amendment of records by the data subject. This exemption is claimed because portions of this system relate to testing or examination materials used solely to determine individual qualifications for appointment or promotion in the Federal Service. Access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or examination process.

(3) Exemptions (a) through (d) are claimed because this system contains investigatory material compiled solely for the purpose of determining suitability, eligibility, and qualifications for Federal civilian employment. To the extent that the disclosure of material would reveal the identity of source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence, the application of exemption(k)(5) will be required to honor such a promise should the data subject request access to or amendment of the record, or access to the accounting of disclosures of the record.

b. Recruiting, Examining, and Placement Records (OPM/GOVT-5).

(1) All information about individuals in these records that meets the criteria stated in 5 USC 552a(k)(5) is exempt from the requirements of 5 USC 552a(c)(3) and (d). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject and access to and amendment of records. These exemptions are claimed because this system contains investigatory material compiled solely for the purpose of determining the appropriateness of a request for approval of an objection to an eligible's qualification for employment in the Federal Service. To the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, the application of exemption (k)(5) will be required to honor such a promise should the data subject request access to the accounting of disclosures of the record or access to or amendment of the record.

(2) All material and information in these records that meets the criteria stated in 5 USC 552a(k)(6) are exempt from the requirements of 5 USC 552a(d), relating to access to and amendment of records by the subject. This exemption is claimed because portions of this system relate to testing or examination materials used solely to determine individual qualification for appointment or promotion in the Federal Service and access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or examining process.

c. Personnel Research Test Validation Records (OPM/GOVT-6). All material and information in these records that meets the criteria stated in 5 USC 552a(k)(6) is exempt from the requirements of 5 USC 552a(d), relating to access to and amendment of the records by the data subject. This exemption is claimed because portions of this system relate to testing or examination materials used solely to determine individual qualifications appointment or promotion in the Federal Service. Access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or examination process.

Table 5-1
Provisions of the Privacy Act from which a general or specific exemption may be claimed

Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(1) Disclosures within the DOD
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(2) Disclosures to the public
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(3) Disclosures for a "Routine Use"
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(4) Disclosures to the Bureau of Census
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(5) Disclosures for statistical research and reporting
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(6) Disclosures to the National Archives
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(7) Disclosures for law enforcement purposes
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(8) Disclosures under emergency circumstances
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(9) Disclosures to the Congress
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(10) Disclosures to the General Accounting Office
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(11) Disclosures pursuant to court orders
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (b)(12) Disclosures to consumer reporting agencies
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (c)(1) Making disclosure accountings
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (c)(2) Retaining disclosure accountings
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (c)(3) Making disclosure accountings available to the individual
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (c)(4) Informing prior recipients of corrections
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (d)(1) Individual access to records
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes

Table 5-1
Provisions of the Privacy Act from which a general or specific exemption may be claimed—Continued

Section of the Privacy Act: (d)(2) Amending records
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (d)(3) Review of the component's refusal to amend a record
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (d)(4) Disclosure of disputed information
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (d)(5) Access to information compiled in anticipation of civil action
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(1) Restrictions on collecting information
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(2) Collection directly from the individual
Exemption (j)(2): Yes Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(3) Informing individuals from whom information is requested
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(A) Describing the name and location of the system
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(B) Describing categories of individuals
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(C) Describing categories of records
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(D) Describing routine uses
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(E) Describing records management policies and practices
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(4)(F) Identifying responsible officials
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(4)(G) Procedures for determining if a system contains a record on an individual
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(4)(H) Procedures for gaining access
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(4)(I) Describing categories of information sources
Exemption (j)(2): Yes Exemption (k)(1&nd: &Yes Section of the Privacy Act: (e)(5) Standards of accuracy
Exemption (j)(2): No Exemption (k)(1&nd: &No Section of the Privacy Act: (e)(6) Validating records before disclosure
Exemption (j)(2): No

Table 5-1
Provisions of the Privacy Act from which a general or specific exemption may be claimed—Continued

<p>Exemption (k)(1)&nd: &No Section of the Privacy Act: (e)(7) Records of First Amendment Activities</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (e)(8) Notification of disclosure under compulsory legal process</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (e)(9) Rules of conduct</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (e)(10) Administrative, technical, and physical safeguards</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (e)(11) Notices for new and revised routine uses</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &Yes Section of the Privacy Act: (f)(1) Rules for determining if an individual is the subject of a record</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &Yes Section of the Privacy Act: (f)(2) Rules for handling access requests</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &Yes Section of the Privacy Act: (f)(3) Rules for granting access</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &Yes Section of the Privacy Act: (f)(4) Rules for amending records</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &Yes Section of the Privacy Act: (f)(5) Rules regarding fees</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (g)(1) Basis for civil action</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (g)(2) Basis for judicial review and remedies for refusal to amend</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (g)(3) Basis for judicial review and remedies for denial of access</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (g)(4) Basis for judicial review and remedies for other failure to comply</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (g)(5) Jurisdiction and time limits</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (h) Rights of legal guardians</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (i)(1) Criminal penalties for unauthorized disclosure</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No</p>

Table 5-1
Provisions of the Privacy Act from which a general or specific exemption may be claimed—Continued

<p>Section of the Privacy Act: (i)(2) Criminal penalties for failure to publish</p>
<p>Exemption (j)(2): No Exemption (k)(1)&nd: &No Section of the Privacy Act: (i)(3) Criminal penalties for obtaining records under false pretenses</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (j) Rulemaking requirement</p>
<p>Exemption (j)(2): N/A Exemption (k)(1)&nd: &No Section of the Privacy Act: (j)(1) General exemption for the Central Intelligence Agency</p>
<p>Exemption (j)(2): N/A Exemption (k)(1)&nd: &No Section of the Privacy Act: (j)(2) General exemption for criminal law enforcement records</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(1) Exemption for classified material</p>
<p>Exemption (j)(2): N/A Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(2) Exemption for law enforcement material</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(3) Exemption for records pertaining to Presidential protection</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(4) Exemption for statistical records</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(5) Exemption for investigatory material compiled for determining suitability for employment or service</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(6) Exemption for testing or examination material</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &N/A Section of the Privacy Act: (k)(7) Exemption for promotion evaluation materials used by the Armed Forces</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (l)(1) Records stored in GSA records centers</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (l)(2) Records archived before September 27, 1975</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (l)(3) Records archived on or after September 27, 1975</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (m) Applicability to Government contractors</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No Section of the Privacy Act: (n) Mailing Lists</p>
<p>Exemption (j)(2): Yes Exemption (k)(1)&nd: &No</p>

Table 5-1
Provisions of the Privacy Act from which a general or specific exemption may be claimed—Continued

Section of the Privacy Act: (o) Reports on new systems

Exemption (j)(2): Yes

Exemption (k)(1) and (k)(2): No

Section of the Privacy Act: (p) Annual report

System name: Out-of-Service Accounts Receivables

System location: U.S. Army Finance and Accounting Center, Ft Benjamin Harrison, IN 46249–1536.

Categories of individuals covered by the system: Separated and retired military/civilian personnel and others indebted to the U.S. Army.

Categories of records in the system: Records of current and former military members and civilian employees' pay accounts showing entitlements, deductions, payments made, and any indebtedness resulting from deductions and payments exceeding entitlements. These records include, but are not limited to:

a. Individual military pay records, substantiating documents such as military pay orders, pay adjustment authorizations, military master pay account printouts from the Joint Uniform Military Pay System (JUMPS), records of travel payments, financial record data folders, miscellaneous vouchers, personal financial records, credit reports, promissory notes, individual financial statements, and correspondence.

b. Applications for waiver of erroneous payments or for remission of indebtedness with supporting documents, including, but not limited to, statements of financial status (personal income and expenses), statements of commanders and/or accounting and finance officers, and correspondence with members and employees.

c. Claims of individuals requesting additional payments for service rendered with supporting documents including, but not limited to time and attendance reports, leave and earnings statements, travel orders and/or vouchers, and correspondence with members and employees.

d. Delinquent accounts receivable from field accounting and finance officers including, but not limited to returned checks, medical services billings, collection records, and summaries of the Army Criminal Investigations Command and/or Federal Bureau of Investigation reports.

e. Reports from probate courts regarding estates of deceased debtors.

f. Reports from bankruptcy courts regarding claims of the United States against debtors.

Authority for maintenance of the system: 31 USC 3711; 10 USC 2774; and 12 USC 1715.

Purpose: To process, monitor, and post-audit accounts receivable, to administer the Federal Claims Collection Act, and to answer inquiries pertaining thereto.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: Information may be disclosed to—

a. U.S. Attorneys, Department of Justice—for legal action or final disposition of the debt claims. The litigation briefs (comprehensive, written referral recommendations) will restructure the entire scope of the collection cases.

b. Internal Revenue Service (IRS)—to obtain locator status for delinquent accounts receivables (automated controls exist to preclude redisclosure of solicited IRS address data), or to report writeoff amounts as taxable income pertaining to amounts compromised and accounts barred from litigation due to age.

c. Private collection agencies—for collection action when the Army has exhausted its internal collection efforts.

Disclosure to Consumer Reporting Agencies: Disclosures pursuant to 5 USC 552a(b)(12) may be made to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 USC 1681a (f)), or the Federal Claims Collection Act of 1966 (31 USC 3701(a)(3)) when an individual is responsible for a debt to the U.S. Army. This is provided the debt has been validated, is overdue, and the debtor has been advised of the disclosure and the right to dispute, appeal, or review the claim; and/or whenever a financial status report is requested for use in the administration of the Federal Claims Collection Act. Claims of the United States may be compromised, terminated, or suspended when warranted by information collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: Paper records in collection file folders and bulk storage; card files, computer magnetic tapes, and printouts; and microfiche.

Retrievability: By SSN, name, substantiating document number and conventional indexing is used to retrieve data.

Safeguards: The U.S. Army Finance and Accounting Center employs security guards. An employee badge and visitor registration system is in effect. Hard copy records are maintained in areas accessible only to authorized personnel who are properly screened, cleared, and trained. Computerized records are accessed by the custodian of the records system and by persons responsible for servicing the record system in the performance of their official duties. Certifying finance and accounting officers of debts have access to debt information to confirm if the debt is valid and collection action is to be continued. Computer equipment and files are located in a separate secured area.

Retention and disposal: Individual military pay records and accounts receivables are converted to microfiche and retained for 6 years. Destruction is by shredding. Retention periods for other records vary according to category, but total retention does not exceed 56 years; these records are sent to the Federal Records Center, GSA at Dayton, Ohio; destruction is by burning or salvage as waste paper.

System manager(s) and address: Commander, U.S. Army Finance and Accounting Center, Indianapolis, IN 46249-1536.

Notification procedure: Individuals desiring to know whether this system of records contains information about them should contact the System Manager, ATTN:FINCP–F, furnishing full name, SSN, and military status, or other information verifiable from the record itself.

Record access procedures: Individuals seeking access to records in this system pertaining to them should submit a written request as indicated in "Notification procedure" and furnish information required therein.

Contesting record procedures: The Army's rules for access to records and for contesting contents and appealing initial determinations are contained in AR340–21(32 CFR, part 505).

Record source categories: Information is received from DOD staff and field installations, Social Security Administration, Treasury Department, financial organizations, and automated systems interface.

Systems exempted from certain provisions of the act: None.

NARRATIVE STATEMENT

1. *System identification and name:* A0404.02DAJA, Courts-Martial Files.
2. *Responsible official:* Mr. James D. Kemper, U.S. Army Legal Services Agency, Office of The Judge Advocate General, Room 204B, Nassif Building, Falls Church, VA 22041-5013.
3. *Purpose of the system:* Records of trial by court-martial are necessary for the purpose of legal review and final action in court-martial cases. After completion of appellate review, they protect each accused against a subsequent trial for the same offense.
4. *Authority for the system:* Title 10 USC, chapter 47, section 865 states that in the case of a general court-martial, or when a sentence that includes a bad-conduct discharge is approved by the convening authority in a special court-martial, the record will be sent to TJAG. All other special and summary courts-martial records will be reviewed by a judge advocate.
5. *Number (or estimate) of individuals on whom records will be maintained:* Approximately 7,000,000.
6. *Information of first amendment activities:* The system contains no information on first amendment activities; the system may include records of trial in which the charged misconduct was an activity protected by the First Amendment.
7. *Measures to assure information accuracy:* In a trial by court-martial, the accused has a unique opportunity to assure that his or her record is accurate, relevant, timely, and complete as it is made. He or she has the right to—
 - a. Be present at trial.
 - b. Be represented by counsel in general and special courts-martial.
 - c. Consult with counsel prior to a summary court-martial.
 - d. Review and challenge all information before it is introduced into evidence.
 - e. Cross-examine all witnesses against him or her.
 - f. Present evidence in his or her behalf.
 - g. Review and comment upon the record of trial before the convening authority's action in general and special courts-martial.
8. *Other measures to assure system security:* As courts-martial records reflect criminal proceedings ordinarily open to the public, copies are normally releasable to the public pursuant to the Freedom of Information Act. However, access to the original records is limited to authorized individuals. Security measures consist of standard physical security devices and civilian and military guards.
9. *Relationship to State/local Government activities:* None.
10. *Supporting documentation:* Proposed system notice and proposed exemption rule are at enclosures 1 and 2, respectively.

Figure 4-2. Sample of a report for a new system of records

Glossary

Section I Abbreviations

AAFES

Army and Air Force Exchange Service

AARA

Access and Amendment Refusal Authority

ACSIM

Assistant Chief of Staff for Information Management

DA

Department of the Army

DOD

Department of Defense

GAO

General Accounting Office

GSA

General Services Administration

JUMPS

Joint uniform military pay system

MACOM

major Army command

MPMIS

Military Police management information system

NARS

National Archives and Records Service

NGB

National Guard Bureau

OMB

Office of Management and Budget

OPM

Office of Personnel Management

SSN

Social Security Number

TAG

The Adjutant General

TIG

The Inspector General

TJAG

The Judge Advocate General

USACIDC

U.S. Army Criminal Investigation Command

Section II Terms

Access

The review of a record or obtaining a copy of a record or parts thereof in a system of records.

Agency

The DOD is a single agency for the purpose of disclosing records subject to The Privacy Act of 1974. For other purposes, including access, amendment, appeals from denials of access or amendment, exempting systems of records, and record-keeping for release to non-DOD agencies, the DA is an agency.

Access and Amendment Refusal Authority

The Army Staff agency head or major Army commander designated sole authority by this regulation to deny access to, or refuse amendment of, records in his or her assigned area or functional specialization.

Confidential source

A person or organization that has furnished information to the Federal Government under an express promise that its identity would be withheld, or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

Data subject

The individual about whom the Army is maintaining information in a system of records.

Disclosure

The furnishing of information about an individual, by any means, to an organization, Government agency, or to an individual who is not the subject of the record, the subject's designated agent or legal guardian. Within the context of the Privacy Act and this regulation, this term applies only to personal information that is a part of a system of records.

Individual

A living citizen of the United States or an alien admitted for permanent residence. The Privacy Act rights of an individual may be exercised by the parent or legal guardian of a minor or an incompetent. (The Privacy Act confers no rights on deceased persons, nor may their next-of-kin exercise any rights for them.)

Maintain

Collect, use, maintain, or disseminate.

Official use

Any action by a member or employee of DOD that is prescribed or authorized by law or a regulation and is intended to perform a mission or function of the Department.

Personal information

Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

Privacy Act request

A request from an individual for information about the existence of, or for access to or amendment of, a record about him or her that

is in a system of records. The request must cite or implicitly refer to the Privacy Act.

Record

Any item, collection, or grouping of information about an individual that—

Routine use

Disclosure of a record outside DOD without the consent of the subject individual for a use that is compatible with the purpose for which the information was collected and maintained by DA. The routine use must be included in the published system notice for the system of records involved.

Statistical record

A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

System manager

The official responsible for policies and procedures for operating and safeguarding a system of records. This official is located normally at Headquarters, DA.

System of records

A group of records under the control of DA from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all systems of records must be published in the *Federal Register*. (A grouping or files series of records arranged chronologically or subjectively that is not retrieved by individual identifier is not a system of records, even though individual information could be retrieved by such an identifier, such as through a paper-by-paper search.)

Section III

Special Abbreviations and Terms

There are no special terms.

Unclassified

PIN 002344-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.59

PIN: 002344-000

DATE: 05-07-99

TIME: 11:23:30

PAGES SET: 25

DATA FILE: s150.fil

DOCUMENT: AR 340-21

DOC STATUS: NEW PUBLICATION