release to that activity. Do not use general

statements, such as “To other federal agen-
cies as required” or “To any other appro-
priate federal agency”.

(j) Polices and Practices for Storing, Retriev-
ing, Accessing, Retaining, and Disposing
of Records in the System:

(k) Storage: State the medium in which DA
maintains the records; for example, in file
folders, card files, microfiche, computer, or a
combination of those methods. Storage does
not refer to the storage container.

(l) Retrievability: State how the Army re-
treives the records; for example, by name,
fingerprints or voiceprints.

(m) Safeguards: Identify the system safe-
guards; for example, storage in safes, vaults,
locked cabinets or rooms, use of guards, vis-
tor controls, personnel screening, computer
systems software, and so on. Describe safe-
guards fully without compromising system
security.

(n) Retention and Disposal. State how long
AR 25–400–2 requires the activity to maintain
the records. Indicate when or if the records
may be transferred to a Federal Records Cen-
ter and how long the record stays there.
Specify when the Records Center sends the
record to the National Archives or destroys
it. Indicate how the records may be de-
stroyed.

(o) System Manager(s) and Address: List the
position title and duty address of the system
manager. For decentralized systems, show
the locations, the position, or duty title of
each category of officials responsible for any
segment of the system.

(p) Notification Procedures: List the title
and duty address of the official authorized to
tell requesters if their records are in the sys-
tem. Specify the information a requester
must submit; for example, full name, mili-
tary status, SSN, date of birth, or proof of
identity, and so on.

(q) Record Access Procedures: Explain how
individuals may arrange to access their
records. Include the titles or categories of of-
ficials who may assist; for example, the sys-
tem manager.

(r) Contesting Records Procedures: The
standard language to use is “The Army’s
rules for accessing records, and for con-
testing contents and appealing initial agency
determinations are contained in Army Regu-
lation 25–71; 32 CFR part 505; or may be ob-
tained from the system manager.”

(s) Record Source Categories: Show cat-
egories of individuals or other information
sources for the system. Do not list confiden-
tial sources protected by 5 U.S.C. 552a(k)(2),
(k)(5), or (k)(7).

(t) Exemptions Claimed for the System: Spe-
cifically list any approved exemption includ-
ing the subsection in the Act. When a system
has no approved exemption, write “none”
under this heading.

APPENDIX G TO PART 505—MANAGEMENT
CONTROL EVALUATION CHECKLIST

(a) Function. The function covered by this
checklist is DA Privacy Act Program.

(b) Purpose. The purpose of this checklist is
to assist Denial Authorities and Activity
Program Coordinators in evaluating the key
management controls listed below. This
checklist is not intended to cover all con-

(c) Instructions. Answer should be based on
the actual testing of key management con-

APPENDIX H TO PART 505—DEFINITIONS

Function

(a) Access. Review or copying a record or
parts thereof contained in a Privacy Act sys-
tem of records by an individual.

(b) Agency. For the purposes of disclosing
records subject to the Privacy Act, Compo-
nents of the Department of Defense are con-

(c) Amendment. The process of adding, de-
leting, or changing information in a system