

Accounting Service which falls within the provisions of 5 U.S.C. 552a(k)(1) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G)-(e)(4)(I) and (f) to the extent that a record system contains any record properly classified under Executive Order 12589 and that the record is required to be kept classified in the interest of national defense or foreign policy. This specific exemption rule, claimed by the Defense Finance and Accounting Service under authority of 5 U.S.C. 552a(k)(1), is applicable to all systems of records maintained, including those individually designated for an exemption herein as well as those not otherwise specifically designated for an exemption, which may contain isolated items of properly classified information

(1) *General exemptions.* [Reserved]

(2) *Specific exemptions.* [Reserved]

Subpart C—Individual Access to Records

§ 324.8 Right of access.

The provisions of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) apply to all DFAS personnel about whom records are maintained in systems of records. All information that can be released consistent with applicable laws and regulations should be made available to the subject of record.

§ 324.9 Notification of record's existence.

All DFAS Privacy Act Officers shall establish procedures for notifying an individual, in response to a request, if the system of records contains a record pertaining to him/her.

§ 324.10 Individual requests for access.

Individuals shall address requests for access to records to the appropriate Privacy Act Officer by mail or in person. Requests for access should be acknowledged within 10 working days after receipt and provided access within 30 working days. Every effort will be made to provide access rapidly; however, records cannot usually be made available for review on the day of request. Requests must provide information needed to locate and identify the

record, such as individual identifiers required by a particular system, to include the requester's full name and social security number.

§ 324.11 Denials.

Only a designated denial authority may deny access. The denial must be in writing.

§ 324.12 Granting individual access to records.

(a) The individual should be granted access to the original record (or exact copy) without any changes or deletions. A record that has been amended is considered the original.

(b) The DFAS component that maintains control of the records will provide an area where the records can be reviewed. The hours for review will be set by each DFAS location.

(c) The custodian will require presentation of identification prior to providing access to records. Acceptable identification forms include military or government civilian identification cards, driver's license, or other similar photo identification documents.

(d) Individuals may be accompanied by a person of their own choosing when reviewing the record; however, the custodian will not discuss the record in the presence of the third person without written authorization.

(e) On request, copies of the record will be provided at a cost of \$.15 per page. Fees will not be assessed if the cost is less than \$30.00. Individuals requesting copies of their official personnel records are entitled to one free copy and then a charge will be assessed for additional copies.

§ 324.13 Access to medical and psychological records.

Individual access to medical and psychological records should be provided, even if the individual is a minor, unless it is determined that access could have an adverse effect on the mental or physical health of the individual. In this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician in accordance with guidance in Department of

Defense 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310).

§324.14 Relationship between the Privacy Act and the Freedom of Information Act.

Access requests that specifically state or reasonably imply that they are made under FOIA, are processed pursuant to the DFAS Freedom of Information Act Regulation. Access requests that specifically state or reasonably imply that they are made under the PA are processed pursuant to this regulation. Access requests that cite both the FOIA and the PA are processed under the Act that provides the greater degree of access. Individual access should not be denied to records otherwise releasable under the PA or the FOIA solely because the request does not cite the appropriate statute. The requester should be informed which Act was used in granting or denying access.

APPENDIX A TO PART 324—DFAS REPORTING REQUIREMENTS

By February 1, of each calendar year, DFAS Centers and Financial Systems Organizations will provide the DFAS Headquarters Privacy Act Officer with the following information:

1. Total Number of Requests for Access:
 - a. Number granted in whole:
 - b. Number granted in part:
 - c. Number wholly denied:
 - d. Number for which no record was found:
2. Total Number of Requests to Amend Records in the System:
 - a. Number granted in whole:
 - b. Number granted in part:
 - c. Number wholly denied:
3. The results of reviews undertaken in response to paragraph 3a of Appendix I to OMB Circular A-130⁴.

APPENDIX B TO PART 324—SYSTEM OF RECORDS NOTICE

The following data captions are required for each system of records notice published in the FEDERAL REGISTER. An explanation for each caption is provided.

1. *System identifier.* The system identifier must appear in all system notices. It is limited to 21 positions, including agency code, file number, symbols, punctuation, and spaces.

⁴Copies available from the Office of Personnel Management, 1900 E. Street, Washington, DC 20415.

2. *Security classification.* Self explanatory. (DoD does not publish this caption. However, each agency is responsible for maintaining the information.)

3. *System name.* The system name must indicate the general nature of the system of records and, if possible, the general category of individuals to whom it pertains. Acronyms should be established parenthetically following the first use of the name (e.g., 'Field Audit Office Management Information System (FMIS)'). Acronyms shall not be used unless preceded by such an explanation. The system name may not exceed 55 character positions, including punctuation and spaces.

4. *Security classification.* This category is not published in the FEDERAL REGISTER but is required to be kept by the Headquarters Privacy Act Officer.

5. *System location.* a. For a system maintained in a single location, provide the exact office name, organizational identity, routing symbol, and full mailing address. Do not use acronyms in the location address.

b. For a geographically or organizationally decentralized system, describe each level of organization or element that maintains a portion of the system of records.

c. For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list each location by category.

d. If multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are published as an appendix to the agency's compilation of systems of records notices in the FEDERAL REGISTER. If no address directory is used, or if the addresses in the directory are incomplete, the address of each location where a portion of the record system is maintained must appear under the 'system location' caption.

e. Classified addresses shall not be listed but the fact that they are classified shall be indicated.

f. The U.S. Postal Service two-letter state abbreviation and the nine-digit zip code shall be used for all domestic addresses.

6. *Categories of individuals covered by the system.* Use clear, non technical terms which show the specific categories of individuals to whom records in the system pertain. Broad descriptions such as 'all DFAS personnel' or 'all employees' should be avoided unless the term actually reflects the category of individuals involved.

7. *Categories of records in the system.* Use clear, non technical terms to describe the types of records maintained in the system. The description of documents should be limited to those actually retained in the system of records. Source documents used only to collect data and then destroyed should not be described.

8. *Authority for maintenance of the system.* The system of records must be authorized by