taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The DCAA organizational element or DoD component that originated the FOUO information shall be informed of its unauthorized disclosure.

(g) Protection of Field Detachment Sensitive Information. (1) Definition. All communication, which qualifies for withholding under Exemptions (2) through (9), between regular DCAA organizational elements and Field Detachment offices is sensitive information and, as a minimum, shall be marked: FOR OFFICIAL USE ONLY (FOUO).

(2) Markings. (i) Communications, which qualify for withholding under Exemptions (2) through (9) initiated by a Field Detachment office, will bear the following marking:

FOR OFFICIAL USE ONLY

Access limited to addressee and his/her designated representative(s) with a need-to-know.

This document may not be reproduced or further disseminated without the approval of the Director, Field Detachment, DCAA.

(ii) All correspondence specifically exempt under Exemptions (2) through (9), including assist audit requests, generated by a regular (non-FD) DCAA office, which is addressed to the Field Detachment, either Headquarters or a field audit office, will be marked FOR OFFICIAL USE ONLY and will be limited within the FAO to one protected office copy.

(3) Storage. (i) All Field Detachment sensitive information in the possession of a regular DCAA office will be stored in a classified container, if available. If a classified container is not available, the sensitive information shall be stored in a locked container controlled by the FAO manager.

(ii) Permanent files currently maintained by regular DCAA offices, which are available to all FAO personnel, should not contain any detailed information on Field Detachment audit interest. That information shall be protected as sensitive information and stored in accordance with paragraph (g)(3)(i) of this appendix.

(4) Dissemination. (i) Access to Field Detachment sensitive information by other DCAA audit and administrative personnel within the office shall be on a strict need-to-know basis as determined by the FAO manager.

(ii) Requests by non-DCAA personnel for access to Field Detachment sensitive information must be coordinated with the Director, Field Detachment, through Headquarters, DCAA.

[56 FR 49685, Oct. 1, 1991, as amended at 60 FR 18006, Apr. 10, 1995; 60 FR 35699, July 11, 1995]

APPENDIX D TO PART 290—AUDIT WORKING PAPERS

(a) *Definition*

(1) Audit working papers contain information from accounting and statistical records, personal observations, the results of interviews and inquiries, and other available sources. Audit working papers may also include contract briefs, copies of correspondence, excerpts from corporate minutes, organization charts, copies of written policies and procedures, and other substantiating documentation. The extent and arrangement of working paper files will depend to a large measure on the nature of the audit assignment.

(2) Working papers are generally classified in two categories: the permanent file and the current file.

(i) Permanent file.

(A) The permanent file on each contractor is a central repository of information gathered during the course of an audit which has continuing value and use to subsequent audits expected to be performed at the same contractor. Permanent files are useful in preparing the audit program and in determining the appropriate scope of subsequent audits. They also provide ready means for auditors to become familiar with the contractor's operations and any existing audit problems or contractor system weaknesses. While summary information on the contractor's organization, financial structure and policies may sometimes be included in permanent files for smaller contractors, such information on large contractors with continuing audit activity is generally maintained in the field audit office at the central reference library.

(B) Items which would logically be included in the permanent file as having continuing value in future audit assignments include:

(*1*) Internal control questionnaire.

(*2*) Internal control review update control log.

(*3*) Vulnerability assessment.

(*4*) MAARs control log.

(*5*) Disclosure statement and revisions in accordance with CAS rules and regulations, and

(*6*) CAS compliance control schedules and a noncompliance summary schedule.

(ii) Current File. The current file usually consists of working papers which have limited use on future assignments. DCAA Forms

7640–19 a, b, and c are the Agencywide Working Paper Indexes and provide a concise summary of items generally found in audit working papers.

(b) *Explanation.*

(1) The preparation of working papers assists the auditor in accomplishing the objectives of an audit assignment. Working papers serve as the basis for the conclusions in the audit report; provide a record of the work done for use as substantiating data in negotiations, appeals, and litigation; provide guidance for subsequent examinations; and serve as a basis for the review and evaluation of the work performed.

(2) Audit working papers are generally prepared at the time audit work is performed and are maintained on a current basis. Working papers normally reflect the progress of the audit and are designed to ensure continuity of the audit effort.

(3) Working papers should be relevant to the audit assignment and not include extraneous pages. Superseded working papers should be clearly marked as such and retained as part of the working paper package.

(4) The nature of audit working papers requires that proper control and adequate safeguards be maintained at all times. Working papers frequently reflect information considered confidential by the contractor and are marked "For Official Use Only" or are classified for government security purposes.

[56 FR 56932, Nov. 7, 1991]

PART 291—DEFENSE NUCLEAR AGENCY (DNA) FREEDOM OF INFORMATION ACT PROGRAM

Sec.

AUTHORITY: 5 U.S.C. 552.

SOURCE: 56 FR 9842, Mar. 8, 1991, unless otherwise noted.

§ 291.1 Purpose.

This part establishes policies and procedures for the DNA FOIA program.

§ 291.2 Applicability.

This part applies to Headquarters, Defense Nuclear Agency (HQ, DNA), Field Command, Defense Nuclear Agency (FCDNA), and the Armed Forces Radiobiology Research Institute (AFRRI).

§ 291.3 Definitions.

(a) *FOIA Request.* A written request for DNA records made by any person, including a member of the public (U.S. or foreign citizen), an organization, or a business, but not including a Federal agency or a fugitive from the law that either explicitly or implicitly invokes the FOIA (5 U.S.C. 552), 32 CFR part 285, 286, or this part.

(b) *Agency record.* (1) The products of data compilation, such as all books, papers, maps, and photographs, machine readable materials or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law in connection with the transaction of public business and in DNA's possession and control at the time the FOIA request is made.

(2) The following are not included within the definition of the word *record:*

(i) Objects or articles, such as structures, furniture, vehicles and equipment, whatever their historical value, or value as evidence.

(ii) Administrative tools by which records are created, stored, and retrieved, if not created or used as sources of information about organizations, policies, functions, decisions, or procedures of a DNA organization. Normally, computer software, including source code, object code, and listings of source and object codes, regardless of medium are not agency records. (This does not include the underlying data which is processed and produced by such software and which may in some instances be stored with the software.) Exceptions to this position are outlined in paragraph (b)(3) of this section.

(iii) Anything that is not a tangible or documentary record, such as an individual's memory or oral communication.

(iv) Personal records of an individual not subject to agency creation or retention requirements, created and maintained primarily for the convenience of an agency employee, and not