REQUEST FOR RECORDS DISPOSITION AUTHORITY

JOB NUMBER: N1-371-02-6

To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION (NWML)
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001

Date received: 8-19-02

1. FROM (Agency or establishment)
Department of Defense

2. MAJOR SUBDIVISION
DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

3. MINOR SUBDIVISION
Manpower, Personnel and Security Directorate

NOTIFICATION TO AGENCY

In accordance with the provisions of 44 U.S.C 3303a, the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE NUMBER	DATE	ARCHIVIST OF THE UNITED STATES
Mr. Thomas Collins, Programs and Oversight Branch (MPS 61)	(703) 681-1341	1-14-03	John W. Carlin

6. AGENCY CERTIFICATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached 9 page(s) are not needed now for the business for this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies.

X☐ is not required ☐ is attached; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
August 6, 2002	Tommie Gregg, Sr. Mr. TOMMIE GREGG, SR.	RECORDS OFFICER/ PRIVACY ACT ADMINISTRATOR

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	(See attached for schedule.) (Chapter V, Supplement I, DISAI 210-15-6, Records Management Manual) **SECURITY RECORDS**		

cc Agency, NR, NWMW

(Chapter V, Supplement I, DISAI 210-15-6, Records Management Manual)

Section I. CLASSIFIED INFORMATION ACCOUNTING AND CONTROL SECURITY FILES

501-06 Reproduction of Top Secret and Special Category Material Files. Forms such as DISA Form 55-1, Request for Reproduction of Top Secret & Special Category Material used to document approval by the originator of Top Secret and Special Category information that the material may be reproduced.

Disposition: Destroy when 2 years old (New).

501-07 Secure Facsimile Header Page Files. Forms such as DISA Form 66-1, Secure Facsimile Header Page used to verify that classified information sent via facsimile was received securely.

Disposition: Destroy when 2 years old (New).

501-09 Policies and Procedures Working Files. Working files and reference copies related to policies and procedures accumulated in offices having agency-wide responsibilities for security. (Note: Use FN 203-01 for Publications Record Sets Files and FN 203-02 for Publications Background Files.)

Disposition: Destroy when 1 year old or when no longer needed for reference, whichever is later (New).

Section II. INFORMATION SECURITY FILES

502-01 Original Classification Authority (OCA) Designation Files. Records such as DISA Form 49, Briefing for DISA Original Classification Authorities relating to justification for and documentation of training required for appointed OCAs.

Disposition: Destroy when superseded (New).

502-02 Agency Information Security Program Data Report. Records such as SF 311, Agency Information Security Program Data Report, submitted to the Information Security Oversight Office (ISOO) annually.

Disposition: Destroy when 2 years old (New).

502-03 Security Classification Guide Files. Records documenting applicable security classification guides.

Disposition: Destroy when superseded (New).

502-04 DOD Security Classification Guide Data Elements Files. Forms such as DD Form 2024, DOD Security Classification Guide Data Elements, submitted to the Defense Technical Information Center (DTIC) to add or correct the DOD database of security classification guides.

Disposition: Destroy 2 years after submission to DTIC (New).

502-05 Mandatory Review for Declassification Files. Records documenting requests to review classified information for mandatory declassification under Executive Order 12958 or predecessor orders or successor orders.

Disposition: Destroy when 2 years old (New).

502-06 Systematic Review Files. Records documenting the review and determination of classification, downgrading, or upgrading of information in accordance with Executive Orders, such as 12958 or predecessor orders or successor orders.

Disposition: Destroy when 2 years old (New).

502-07 Security Classification Challenges Files. Requests received and decisions made regarding the classification of material individuals believed to be improperly classified.

Disposition: Destroy when 2 years old (New).

502-08 Maintenance and Operating Inspection Files. Documentation of the repair and maintenance of classified material security containers and vaults noted in records such as DISA Form 189 or Optional Form 89, Maintenance Record for Security Containers/Vault Doors.

Disposition: Destroy when 2 years old (New).

502-09 Courier Files. Records such as DD Form 2501, Courier Authorization, DD Form 1610, Request and Authorization for TDY Travel of DOD Personnel; or courier

authorization letters documenting the training of individuals and related information regarding issuance of courier letters/cards to individuals authorized to hand-carry classified information.

Disposition: Destroy when 2 years old (New).

502-10 Security Education and Training Files. Records such as documentation of individuals receiving initial, foreign travel, counterintelligence, refresher, and termination briefings.

Disposition: Destroy when 2 years old (New).

502-12 Security Discrepancy Notice Files. Records such as DISA Form 26, Security Discrepancy Notice, which are sent to organizations outside of DISA to inform them of classified information that has been improperly transmitted, packaged, classified, contained improper markings, and/or other violations of DOD regulation(s).

Disposition: Destroy when 2 years old (New).

502-13 Security Manager Appointment Files. Records relating to appointments of individuals designated to serve as organizational Security Managers.

Disposition: Destroy when superseded (New).

502-14 Security Manager's Meeting Minutes Files. Records such as agendas and minutes of periodic Security Manager's Meetings.

Disposition: Destroy when superseded (New).

502-15 Self-Inspection Files. Records such as annual self-inspections conducted to evaluate and assess the effectiveness and efficiency of the component's implementation of the DOD Information Security program.

Disposition: Destroy when superseded (New).

502-16 Standard Operating Procedure (SOP) Files. Records such as SOPs created for policies and procedures unique to the organizational element.

Disposition: Destroy when superseded (New).

Section III. PHYSICAL SECURITY FILES

503-01 Employee Temporary Badge Log Files. Records such as DISA Form 200, Employee Temporary Badge, used to maintain accountability of temporary access cards issued to employees.

Disposition: COFF: Monthly. Destroy 3 months after cutoff (New).

503-02 Report of Lost DISA and/or Other Affiliated Badges. Records such as DISA Form 23, Report of Lost DISA and/or Other Affiliated Badges, used to record individual reports of lost badges.

Disposition: COFF: Annually. Destroy 1 year after COFF. (New).

503-04 Visit Notification Files. Records such as DISA Form 43, Visit Notification, completed by DISA personnel and verified by organizational Security Managers notifying activities outside DISA of the activity to be visited which provides personal and clearance information.

Disposition: Destroy upon completion or cancellation of visits (New).

Section V. PERSONNEL SECURITY CLEARANCE FILES

Records accumulating from investigations of personnel conducted under Executive Orders and statutory or regulatory requirements.

505-05 Security Termination Statement Files. Records such as DISA Form 553, Security Termination Statement, that officially document an individual's decision to terminate their employment, contract, and/or affiliation with DISA. (Note: These records are in addition to records on termination or separation that appear in personnel files under File Numbers 601-03 and 603-01.)

Disposition: Destroy when 2 years old (New).

Section VI. COMMUNICATION SECURITY FILES

506-03 COMSEC Material Official Inventory Files. Official inventories received semi-annually from the National Security Agency (NSA) for auditing purposes.

Disposition: Destroy after 2 years (New).

506-04 COMSEC Material Transfer, Destruction, and Hand Receipt Files. Records such as Standard Form 153, COMSEC Material Report, reflecting the transfer of material into and out of the COMSEC account. Includes documenting hand receipt of material to authorized users and official destruction of controlled material.

Disposition: Destroy after 2 years (New).

506-05 COMSEC Responsible Officer Appointment Letters. Records such as letters appointing individuals the authority to handle receipt of COMSEC material. Also included are the Cryptographic Access Briefing and Cryptographic Access and Termination forms for each authorized person.

Disposition: Destroy when superseded (New).

Section VII. SPECIAL ACCESS/SENSITIVE COMPARTMENTED INFORMATION (SCI) FILES

This section pertains to SCI - classified information derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of Central Intelligence.

507-01 SCI Officials Files.

Records documenting the appointment of Special Security Officer (SSO) who provides SCI advice and assistance and has day-to-day SCI security cognizance over their offices and subordinate Sensitive Compartmented Information Facilities (SCIFs).

Disposition: Destroy when superseded (New).

507-02 Special Security Representative (SSR) Appointment Files. Records documenting the appointment of SSRs who are responsible for the day-to-day management and implementation of SCI security and administrative instructions for separate, subordinate Sensitive Compartmented Information Facilities (SCIFs).

Disposition: Destroy when superseded (New).

507-03 Self-Inspection Files. Records of self-inspections of DISA security programs conducted at least annually.

Disposition: Destroy when superseded (New).

507-04 Inspection Files. Records documenting the inspections conducted by the Defense Intelligence Agency (DIA) conducted periodically.

Disposition: Destroy when superseded (New).

507-05 Compartmented Address Book (CAB) Files. Records documenting the changes submitted to the CAB, including servicing organization, message address, collateral address, pouching address, Defense Courier Service (DCS) addressing element, telephone numbers (DSN and commercial), accreditation level, supported elements, and special instructions.

Disposition: Destroy when superseded (New).

507-06 SCI Access Management Files. Record of all SCI indoctrinations and debriefings (DD Forms 1848, Debriefing Memorandum) when the need-to-know has ceased or an individual's SCI is terminated for cause). Number of accesses (by compartment) granted, denied, revoked, and suspended. Identification of an individual's Director of Central Intelligence (DCID) 1/14 eligibility date, Single Scope Background Investigation (SSBI) date, SCI Nondisclosure Agreement (NDA) date, accesses, and waivers.

Disposition: Destroy 2years after debriefing of individual (New) .

507-08 Inadvertent Disclosure Briefing Files. Records that reflect briefing and signature of individual(s) (and witnesses) who may have inadvertently been exposed to Sensitive Compartmented Information (SCI).

Disposition: Destroy after 70 years (New).

507-09 Compelling Need Request Files. Requests for access in exceptional circumstances based on the compelling need of an organization to prevent failure or serious impairment of missions or operations that are in the best interest of the national security.

Disposition: Destroy once action is completed and person is briefed to meet the mission requirement (New).

507-10 Access by Other Individuals Files. Requests for SCI access for special purposes by former senior DOD officials, individuals on detail/temporary duty, reserve personnel, contractors, and consultants.

Disposition: Destroy 1 year after request is acted on or when no longer needed, whichever is later (New).

507-11 Transfer in Status (TIS) Files. Requests and other material related to individuals transferring from one DOD component, command, or activity to another DOD component, command, or activity in a SCI-indoctrinated status.

Disposition: Destroy 1 year after receipt of comeback or TIS request (New).

507-12 Periodic Reinvestigation (PR) Files. Documentation of programs established to ensure PRs are conducted in accordance with CIA guidance such as Directive 1/14.

Disposition: Destroy 2 years after departure of the individual (New).

507-13 Personnel Security Eligibility Files.

Files maintained on each SCI-indoctrinated person, such as notifications of any significant changes in their personal status that may adversely affect their continuing eligibility for SCI access.

a. Personnel security files.

Disposition: Destroy 2 years after the debriefing of the individual and/or accountability of the person ceases (New).

b. Justifications for SCI access approval/disapproval.

Disposition: Destroy 2 years after the debriefing of the individual (New).

507-17 Physical Security of Sensitive Compartmented Information Facilities (SCIF) Files.

Documentation of concept approval, pre-construction approval, and accreditation of SCIF.

Disposition: Destroy 2 years after de-certification of SCIF (New).

507-18 Emergency Action Plans (EAP) Files. Plans for emergency situations Plans for emergency situations that occur in SCIFs such as power outages, alarm outages, hazardous material threats, a serious injury, and/or illness.

Disposition: Destroy when superseded or SCIF is decertified, whichever is sooner (New).

507-19 Visitor Control Files. Written procedures and other records for identifying and controlling visitors into the SCIF. Included are access rosters and visit certifications such as DISA Form 269, Sensitive Compartmented Information Facility (SCIF) Visitor Log.

Disposition: Destroy 1 year after the date of the last entry or when procedures are superseded, whichever is applicable (New).

507-20 Technical Surveillance Countermeasures (TSCM) Surveys and Evaluations Files. Records regarding physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at technical penetration.

Disposition: Destroy when superseded or when facility is decertified, whichever is sooner (New).

507-21 Special Access Program (SAP) Files. Records maintained by a DISA program or activity to manage enhanced security measures exceeding those normally required for collateral information of the same classification level when it is determined that normal security measures may be insufficient to protect the information from unauthorized disclosure.

Disposition: Destroy 1 year after the particular SAP is terminated (New).

507-22 Special Access Briefing Files. Documentation of briefings and list of personnel briefed for special accesses such as Critical Nuclear Weapons Design Information (CNWDI), Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).

Disposition: Destroy 2 years after access has been terminated (New).

Section VIII. ELECTRONIC COPIES

508-01 Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the record keeping copy are made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Disposition: Destroy/delete within 180 days after the recordkeeping copy has been produced (New).

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Disposition: Destroy/delete when dissemination, revision, or updating is completed (New).