REQUEST FOR RECORDS DISPOSITION AUTHORITY

(See Instructions on reverse)

TO NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR)
WASHINGTON, DC 20408

1 FROM (Agency or establishment)
Office of the Inspector General

2 MAJOR SUBDIVISION
Department of Defense

3 MINOR SUBDIVISION
OIG for Investigations, Defense Criminal Investigative Service

4 NAME OF PERSON WITH WHOM TO CONFER
Retta Graham-Hall, Records Manager

5. TELEPHONE
(703) 604-9781

VE BLANK (NARA use only)

JOB NUMBER
N1-509-05-1

DATE RECEIVED
10-25-2004

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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10

DATE
3/15/06

ARCHIVIST OF THE UNITED STATES
Allen Weinstein

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 4 page(s) are not now needed for the business of 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,

☒ is not required; ☐ is attached, or ☐ has been requested

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
9/23/2004	Jonilyn M Palachuk	Director, Administration & Logistics Services Directorate

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	THIS REQUEST FOR RECORDS DISPOSITION AUTHORITY COVERS RECORDS FOR THE OFFICE OF THE INSPECTOR GENERAL DEPARTMENT OF DEFENSE OFFICE OF THE DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS which are not covered by the NARA General Records Schedule OR previously approved records schedules for the Defense Criminal Investigative Service Please see the attached 4 pages Love A. Silverthorn DATE. 8/30/04 Concurred with on this date by Love Silverthorn, Investigative Review Specialist, DCIS Jon Karanian DATE 9/20/04 Concurred with on this date by the Office of the General Counsel OIG cc Agency NR NWMW NWCT		

NSN 7540-00-634-4064
PREVIOUS EDITION NOT USABLE

RECORDS SCHEDULE FOR THE RECORDS OF THE

Inspector General, Department of Defense
Sources Program
in the office of the
Defense Criminal Investigative Service

The Defense Criminal Investigative Service (DCIS) is headed by the Director, DCIS under the Deputy Inspector General for Investigations, Office of the Inspector General, Department of Defense.

DCIS MISSION

DCIS' mission is to protect America's warfighters by conducting investigations in support of crucial National Defense priorities. DCIS assists the Inspector General in fulfilling statutory responsibilities to detect, investigate and prevent fraud, waste and abuse and other improper acts. To this end, DCIS investigates allegations of criminal, civil and administrative violations and promotes economy, efficiency and effective operations within DoD. Pursuant to the statutory obligations of the DoD Inspector General to "initiate, conduct, and supervise such . . . investigations in the Department of Defense (including the military departments) as the Inspector General considers appropriate" (IG Act §8(c)(2)) and to "give particular regard to the activities of the internal ... investigative units of the military departments with a view toward avoiding duplication and insuring effective coordination and cooperation" (IG Act §8(c)(9)), the DCIS devotes the majority of its' resources to investigations involving terrorism, product substitution, computer crimes/intrusions, illegal technology transfers, and other categories of fraud (i.e. bribery, corruption, and major thefts).

INVESTIGATIVE OPERATIONS

Investigative Operations Directorate includes four major programs: National Security, Special Operations, Economic Crimes, and Technical Operations.

The Special Operations Program is responsible for conducting undercover operations, case-based oversight projects based on Congressional requests, requests from within the Defense Department's investigative community, or proactive initiatives.

SOURCE PROGRAM

The purpose of the DCIS Source Program (initiated in 1980) is to:

a. Obtain information containing data about personnel who have been used as sources of criminal information by DCIS, details on use or activities of source that are necessary to confirm operational use as source, or future claims against DCIS by source or heirs of source.
b. May contain agreements, fingerprints, contracts, information and financial reports and related information.
c. Provide an additional means for a coordinated evaluation of administrative, civil, and criminal actions appropriate to the situation.

The Source Program was created to establish, manage, and administer control of all sources. The use of sources is to collect information and identify substantive criminal activities. Sources are utilized to collect information and identify substantive criminal activities. It is a means by which DCIS agents can bring to light potential civil or criminal matters. Therefore it is necessary for the development of sources to fulfill the mission and objectives of the Office of the Inspector General of the Department of Defense.

Attached is a pamphlet entitled "Source Program," which provides a description of the process that provides applicable general guidelines, policy and procedures.

SOURCE PROGRAM

The Headquarters Defense Criminal Investigative Service's (DCIS) Source Control Officer maintains all original sources documents (confidential and registered) acquired by DCIS personnel through investigations. Sources provide criminal information used for DCIS investigations.

1. Source Program Management and Policy Files

The DCIS Special Agents Manual Chapter 7, "Sources," deal with issues relating to Program implementation, and execution and issues that arise during the normal course of the Source Program. Files do not relate exclusively to a particular source and investigative case or possible future investigation. Files consist of, but are not limited to, internal (OIG-DCIS) and external correspondence establishing the Source program, correspondence with DCIS agents, yearly source reports submitted by the field source control officer on specific issues of program, yearly reports. Most, if not all, of the program management and policy files remain within Investigations. Program Management files are opened and maintained for general matters of program policy and program administration and admission decisions.

Source Program Management and Policy Files exist from 1980 to present Files are created as change in program or policy issues arise.

Volume: Approximately .5 file drawers. Estimated annual growth is approximately .5 file drawer.

Files are referenced daily.

DISPOSITION:

a. PERMANENT. Create new file folder as issues arise. Retain in the Headquarters Source Program Office ~~or~~ as long as the policy/procedure is currently in effect, whichever is longer, then transfer to Washington National Records Center (WNRC). Transfer to the National Archives 25 years after closure or renewal of policy file.

b. Electronic mail and word processing system copies.

(1) Copies that have no further administrative value after the recordkeeping 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. DELETE within 180 days after the recordkeeping copy has been produced.

(2) Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. DELETE when dissemination, revision, or updating is complete.

2. Source Files

Contain but are not limited to material dealing with the specific source file. Each source has a specific file that is identified by a unique field office source control number. The source file may relate to a specific investigative case or possible future investigation but may NEVER be placed in a case file in order to protect the source. Each file contains, but is not limited to, correspondence from field reports and notes. It may contain an agreement; fingerprints; polygraph; source status reports; any payments made to source; correspondence between the HQ SCO and the Office of General Counsel, DoD; and the U.S. Attorney's Office.

Files are created when a new source data report (SDR) is received from the field office identifying a new source to the Program or a transferred source from one field office to another. A source file is closed when the HQ SCO receives the final SDR. The source file is retained for 2 years from case closure with the HQ SCO and than transferred to the WNRC. Files are established/created and closed on a fiscal year basis.

Currently there are 1865 sources that date back to 1980.

Volume: Approximately 5 file drawers. The estimated annual growth is approximately 1 file drawer

The closed source files are rarely referenced.

DISPOSITION:

A. TEMPORARY: Create a new file each time a new source is established. Close file by the exact date of the Fiscal Year in which the final SDR was written. Retire all Source files that are identified by a field office internal source control to Washington National Records Center (WNRC) three (3) years after receipt at INV-HQ of original/ final SDR from the field office. Destroy 25 years after case closure to coincide with destruction of associated investigation.

B. PERMANENT. Create a new file each time a new source is established. Close file by the exact date of the Fiscal Year in which the final SDR was written. Retire all Source files that are identified by a field office internal source control number to the Washington National Records Center three (3) years after receipt at INV-HQ of original/final SDR from the field office. Transfer to the National Archives 25 years after case closure **ONLY** if the source files were established in conjunction with an investigation that meets one or more of the following criteria:

Investigative case files in Case Categories:

F – Redistribution/Marketing Fraud; **O** - U.S. Customs Violations;
S – Environmental; **T** – Terrorism Related Act;
W - Computer Intrusion; and **X** - Internal Security

And/or, any cases that:

1. Establish a precedent and result in a major policy or procedural change;
2. Are involved in extensive litigation;
3. Receive widespread news media attention;

4. Widely recognized for uniqueness by specialists or authorities outside the Government;
5. Reviewed at length in the Agency's annual report to Congress.

C. Electronic mail and word processing system copies

(1) Copies that have no further administrative value after the recordkeeping 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. DELETE within 180 days after the recordkeeping copy has been produced.

(2) Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. DELETE when dissemination, revision, or updating is complete.