

REQUEST FOR RECORDS DISPOSITION AUTHORITY		JOB NUMBER <i>NI-065-07-17</i>	
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001		Date received <i>8/20/07</i>	
1 FROM (Agency or establishment) DEPARTMENT OF JUSTICE		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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10	
MAJOR SUBDIVISION FEDERAL BUREAU OF INVESTIGATION			
MINOR SUBDIVISION RECORDS MANAGEMENT DIVISION			
4. NAME OF PERSON WITH WHOM TO CONFER Teresa C. Sharkey, CRM	TELEPHONE NUMBER 202-324-1613	DATE <i>8/14/09</i>	ARCHIVIST OF THE UNITED STATES <i>Adrienne Thomas</i>
<p>AGENCY CERTIFICATION</p> <p>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 <u>3</u> 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,</p> <p><input checked="" type="checkbox"/> is not required <input type="checkbox"/> is attached, or <input type="checkbox"/> has been requested</p>			
DATE <i>8/13/07</i>	SIGNATURE OF AGENCY REPRESENTATIVE <i>William L. Hooton</i>		TITLE Assistant Director
7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	The attached pages provide disposition instructions for records relating to the Document Capture System (DCS), which is a system used to manage the administrative scanning processes of the FBI's records and evidence		

Document Capture System (DCS)

The Document Capture System (DCS) is an Oracle system developed in 2004 for the Federal Bureau of Investigation's (FBI's) Records Management Division's Document Conversion Laboratory (DocLab). The DocLab scans records and evidence for the FBI and uses DCS to automate and manage the DocLab's processes, which include logging incoming requests for services, receiving documents to be scanned, document preparation, scanning, quality assurance, job completion and verification, and delivery of the scanning job.

1. INPUTS

a. Source Records, FBI Records/Case Files (hard copies to be scanned by the DocLab)

These records primarily include, but are not limited to records being scanned for use in the Freedom of Information and Privacy Act (FOIPA) and name check processes and scanning related to the FBI's case work.

DISPOSITION: RETAIN/DESTROY commensurate with the disposition authorities approved in N1-065-82-04 and N1-065-04-4.

b. Source Records, Evidence (hard copies to be scanned by the DocLab)

DISPOSITION: Disposition is based on the rules of evidence.

c. Job Information

These records include job information the DocLab needs in order to process a new scanning job. Data is keyed into the system that includes, but is not limited to job name, division name, tracking number, output media, priority, case title, classification, date received, and correspondence log information.

DISPOSITION: see "Data Files"

d. Job Information, Supporting Records (hard copy)

These records include instructional memos, notes and other information regarding processing the job, which are scanned and uploaded into the system.

DISPOSITION: DELETE/DESTROY after verification of a successful scan.

e. Employee Statistical Data

This information includes keyed in data of employee statistics, e.g. the employee name, the date and the quantity of pages scanned.

DISPOSITION: see "Data Files"

f. Employee Statistical Data Input Worksheets/Forms (hard copy)

These records include, but are not limited to worksheets, forms, and other records that have employee statistical data that is keyed into DCS.

DISPOSITION: DELETE/DESTROY after verification of successful data input.

2. DATA FILES

a. Image Data Files (Images of Source Records)

These records are the images of the scanned hard copies

DISPOSITION DELETE/DESTROY 90 days after the customer copy and the back-up copies are created

b. Job Processing Data & Metadata

This information about each job being processed including, but not limited to bar code information, quantity of pages scanned in an individual job, box, and unit, the day and time when a process, such as scanning begins and ends, name of employee processing job, and information on when a job is received or shipped back to a customer

DISPOSITION DELETE/DESTROY three years after completion of the job or when no longer needed for administrative purposes, whichever is later

c. Job Information & Supporting Records Data

This information includes information about the job, i.e. the job name, division name, tracking number, output media, priority, case title, classification, date received, and correspondence log information

DISPOSITION DELETE/DESTROY one year after completion of the job (~~GRS 13, 2a~~) or when no longer needed for administrative purposes, whichever is later

3. OUTPUTS

a. Statistical Reports

These records include, but are not limited to standard and ad hoc graphs and reports, e.g. image count reports, individual job detail reports, employee production data, and job statistical reports

DISPOSITION DELETE/DESTROY when 3 years old or when no longer needed for administrative purposes, whichever is later

b. Job Processing Records

These records include, but are not limited to the records and information output from the system that enable the processing of each job, e.g. bar code labels, worksheets

DISPOSITION DELETE/DESTROY one year after completion of the job (~~GRS 13, 2a~~) or when no longer needed for administrative purposes, whichever is later

c. Images, Customer Copy (Images of Source Records)

These records are the images of the source files

DISPOSITION DELETE/DESTROY images of records and evidence in accordance with the FBI's records retention policies, practices, and the rules of evidence

4. DOCUMENTATION

System Documentation

Includes system specifications, file specifications, codebooks, user guides, output specifications, and final reports

DISPOSITION DELETE/DESTROY when superseded or obsolete, or upon authorized deletion of the related master file or database or upon the destruction of the output of the system, if the output is needed to protect legal rights, whichever is latest

5. RELATED RECORDS

a. Job Information Records (hard copy)

These records were created prior to DCS and include forms, electronic communications (ECs), notes, etc regarding the instructions of completed job requests

DISPOSITION DELETE/DESTROY one year after completion of the job ~~(GRS 13, 2a)~~

b. Images, DocLab's Back-Up Copies

These records are the back-up copies created by the DocLab at the time the images are placed on the customer's requested medium. The back-up customer copy is retained by the DocLab to assist in servicing the same request. In addition, the back-up copy serves as a short-term back-up copy should there be any problems in the delivery of the medium to the customer.

DISPOSITION DELETE/DESTROY when 90 days old

GRS 20, item 8

c. Customer Service Feedback & Related Information

These records include, but are not limited to customer satisfaction surveys, feedback questionnaires, and reports generated based on customer feedback.

DISPOSITION DELETE/DESTROY one year after the year in which the project is closed (GRS 16, 5) or when no longer of administrative value, whichever is later.

d. System Backup Files

A full backup is performed nightly and maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

DISPOSITION DELETE/DESTROY incremental backups when superseded by a full backup or when 90 days old

DELETE/DESTROY full backups when a more current full backup has been successfully captured or when 90 days old

GRS 24, item 4

e. Security Audit Logs

Oracle audits are performed that capture database-specific events, including logins, accesses, and administrative activities.

DISPOSITION DELETE/DESTROY electronic files and hard-copy printouts created to monitor system usage, when no longer needed for administrative, legal, audit, or other operational purposes ~~(GRS 20, item 1c)~~