

REQUEST FOR RECORDS DISPOSITION AUTHORITY		JOB NUMBER N1-065-09-15	
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001		Date received 5/13/09	
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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10	
2 MAJOR SUBDIVISION Federal Bureau of Investigation			
3 MINOR SUBDIVISION Counterintelligence Division			
4. NAME OF PERSON WITH WHOM TO CONFER Tammy J. Strickler	5 TELEPHONE NUMBER 540-868-4363	DATE 14 Jun 10	ARCHIVIST OF THE UNITED STATES
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 <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, <input checked="" type="checkbox"/> is not required <input type="checkbox"/> is attached, or <input type="checkbox"/> has been requested			
DATE 5/4/2009	SIGNATURE OF AGENCY REPRESENTATIVE 		TITLE Chief, Records Automation Section (for) Agency Records Officer
7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	The Federal Bureau of Investigation's (FBI's) Surveillance Technology and Architecture Renewed Desktop (STandARD) application was implemented in 2006, but contains data that was migrated into the system from the previous system that was used until 2009. Surveillance Specialists enter data (e.g. about visitors, even if the name is unknown) and surveillance photographs into STandARD that relate to surveillance of Lookout platforms, such as trade shows, controlled meets, special events, and foreign establishments such as embassies.		

Surveillance Technology and Architecture Renewed Desktop (STandARD)

PURPOSE

The Federal Bureau of Investigation's (FBI's) Counterintelligence Division is responsible for the Surveillance Technology and Architecture Renewed Desktop (STandARD) application was implemented in 2006, but contains data that was migrated into the system from the previous system that was used until 2009. Surveillance Specialists enter data (e.g. about visitors, even if the name is unknown) and surveillance photographs into STandARD that relate to surveillance of Lookout platforms, such as trade shows, controlled meets, special events, and foreign establishments such as embassies.

The application is an Oracle 10g database with a PowerBuilder front end that also has a Java interface, which is used to manage the importing of still image surveillance photographs. Along with the photographs, the application contains information on subjects, unknown persons, and vehicles observed during surveillances. Each observation is noted with its respective date and time. Records contained in the system are classified at Secret and below.

A. INPUTS

1. Keyed in Data

These records include data input into the system, including but not limited to name, nickname, sex, also known as name(s), date of birth, age, age range, establishment, date of arrival, expected length of stay, photograph information (photograph date and photograph caption), vehicle information (car make, car plate), case file information, case agent, spouse information, children information, and surveillance information (derived by, declassified on, physical surveillance of, date, file number, time, initials, and observations).

DISPOSITION See Data Files (B item 1)

2. Sources of Keyed in Data

These source records include but are not limited to handwritten notes, information obtained from other FBI systems or other agencies, and records used during surveillance. Data from the records is input into STandARD.

DISPOSITION Delete/Destroy after data has been successfully keyed into STandARD

GRS 20

3. Photographic Images and Metadata

These records include relevant camera and video surveillance still image photographs that are uploaded into STandARD along with any related metadata about the photos, such as type (photo), source, and caption. (Note the system is capable of supporting the attachment of multimedia files.)

DISPOSITION See Data Files (B item 1)

4. Previous System Data

This information includes data that was used in the system used prior to STandARD. The data input is consistent with the type of information defined in Keyed in Data (A item 1).

DISPOSITION See Data Files (B item 1)

5. Look-Up Table Information

This information includes data imported into the system that is used to standardize input and expedite data entry, such as information related to vehicle makes and models, establishment names, etc.

DISPOSITION Delete/Destroy when data is superseded or no longer of value

B. DATA FILES

1. Surveillance Data Files

These files are comprised of the information and records uploaded into the system, as described in Inputs and all related images and metadata

DISPOSITION Data File Cut-off end of calendar year the data was entered into the system
Delete/Destroy 25 years after the Data File Cut-off

2. Look-Up Table Data

This information is used for research and/or to populate a field of information within the system and includes, but is not limited to make and model information

DISPOSITION Delete/Destroy when superseded or no longer of administrative value, whichever is sooner

C. OUTPUTS

1. Reports/Information Related to an FBI Investigation

These records include information in the form of reports and graphs that relate to activities by person, activities by vehicle, daily activity reports and daily logs that show who came and went, etc

DISPOSITION Retain/Destroy commensurate with the case file

File instruction

2. Statistical Reports

These records include standard and ad hoc reports used for administrative, inspection, or management purposes Any STandard and/or ad hoc reports produced by STandard are not saved within the application, but the report would be saved to a file location chosen by the user

DISPOSITION File Cut-off end of each calendar year
Delete/Destroy 2 years after File Cut-off

D. DOCUMENTATION

Records include system specifications, file specifications, codebooks, user guides, and output specifications

DISPOSITION Destroy/delete 1 year after termination of the system (Changed to reflect standardized disposition as reflected in 319U5)

GRS 20

E. RELATED RECORDS

1. Surveillance Records

The images are created from both cameras and video surveillance tapes, which are recorded on various formats/media (e.g. 6mm, 8mm, VHS, etc)

a. Photographs, Media Deemed Relevant

DISPOSITION Retain/Destroy commensurate with the case file

File instruction

b. Footage, Photographs, Media Deemed Not Relevant

DISPOSITION Delete/Destroy after successful import/upload of relevant photos

2. Previous System

These records include the system, audit logs, user manuals and any other related system metadata and system records

DISPOSITION Delete/Destroy four (4) years after successful migration of relevant data into STandard

(This migration of data is ongoing, and expected to be completed by December 31, 2009)

3. **System Backup Files**

These files include backup tapes that are 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

Delete/Destroy full backups when a more current full backup has been successfully captured

GRS 24

4. **Audit Logs**

These records include audit logs relating to application events (errors, warning or information that programs generate), security events (something that affects the security of the entire system), system events (errors, warning and information that is generated by the Windows workstation components)

Disposition Cut-Off upon system termination or upon migration of system data, including audit logs to another system, whichever is sooner

Delete/Destroy 25 years after cut-off