REQUEST FOR RECORDS DISPOSITION AUTHORITY

<table>
<thead>
<tr>
<th>JOB NUMBER</th>
<th>N1-065-09-10</th>
</tr>
</thead>
</table>

To NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADEPHI ROAD COLLEGE PARK, MD 20740-6001

Date received 5/13/09

1 FROM (Agency or establishment)
   Department of Justice

2 MAJOR SUBDIVISION
   Federal Bureau of Investigation

3 MINOR SUBDIVISION
   Counterterrorism Division

4 NAME OF PERSON WITH WHOM TO CONFER
   Tammy J Strickler

5 TELEPHONE NUMBER
   540-868-4363

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 2 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 4/4/2009
   SIGNATURE OF AGENCY REPRESENTATIVE

   TITLE Chief, Records Automation Section
   (for) Agency Records Officer

7 ITEM NO

8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION
   The Guardian Threat Tracking System.
   The Federal Bureau of Investigation (FBI) established the Guardian Threat Tracking System (hereinafter referred to as “Guardian”) to manage terrorist threat and/or suspicious activities having a possible nexus to terrorism. The information in Guardian comes from information provided by other government agencies and private citizens.

9 GRS OR SUPERSEDED JOB CITATION

10 ACTION TAKEN (NARA USE ONLY)

115-109 PREVIOUS EDITION NOT USABLE

STANDARD FORM 115 (REV 3-91)
Prescribed by NARA 36 CFR 1228
Guardian Threat Tracking System

Guardian is a database application that contains records of terrorist threat information and/or suspicious activities having a possible nexus to terrorism, as well as the results of investigative activity. The information in Guardian comes from information provided by other government agencies and private citizens. Guardian contains real-time data.

Any urgent report sent to the Counterterrorism Division (CTD) of the Federal bureau of investigation (FBI) regarding a terrorism-related event, terrorist threat, or suspicious activity is entered into Guardian. In addition, information that would typically be reported as a complaint (FD-71) or would be forwarded to a CTD squad is entered into Guardian. Generally, items entered and updated in Guardian are those activities, incidents, or observations that may have a nexus to terrorism and should be either (1) actionable as an individual entry, (2) useful in establishing a pattern of questionable behavior, or (3) beneficial in a post-incident investigation or analysis.

Guardian was modeled upon the FBI Baltimore Division's Baltimore Terrorism Tracking System (BaTTS) and the Terrorist Activity Reporting Tool (TARS). The primary purpose of Guardian is to create an FBI-wide collection of terrorism information related referrals, including those from the public and other agencies, and to share this information throughout the FBI.

Disposition:

1. Inputs: Information is keyed directly into Guardian, or uploaded from external media. 

   Disposition: DELETE/DESTROY any paper/electronic sources for inputs within 180 days of verification of successful entry to Guardian.

2. Data Files: Guardian entries may contain either specific and actionable information with a possible nexus to terrorism, or information with no unique and actionable identifiers, but which may be useful in pattern analysis.

   a. Non-actionable intelligence. Information entered into the system that contains no nexus to terrorist activity or pattern-based analysis.

   Disposition: DELETE/DESTROY 5 years after entry into Guardian, as per 28 CFR Part 23.

   b. Actionable intelligence:

   Disposition: DELETE/DESTROY 30 years after incident closure or when no longer needed for analytical purposes, not to exceed the life of the system. A copy of Guardian data is uploaded directly to the Automated Case Support (ACS) (successor system SENTINEL) system via FBI Form 71A, once an incident is closed.

   FORMER CASE FILE
   FBI 7/19/04
   11/10/01
3. Outputs: Guardian users may obtain responses or "hits" that provide information useful to a current investigation or intelligence gathering activity.

a. Queries

Disposition: DELETE/DESTROY results of queries 30 years after the date of the query.

b. Investigative and Intelligence Leads

Leads and other information that are used for investigative or intelligence purposes are incorporated into the related FBI investigative or intelligence case file.

Disposition: RETAIN/DESTROY commensurate with the retention period approved for the related file classification.

4. System Documentation:

Specifications, design criteria, codebooks, record layouts, user guides, search tools and their dates of usage, change management requests, data dictionaries, and related information.

Disposition: DELETE/DESTROY when superseded or obsolete, or upon authorized deletion of the related data set.

Related Records:

5. Usage Agreements and Memoranda of Understanding:

Disposition: DELETE/DESTROY when superseded or obsolete or upon termination of Guardian, whichever is sooner.

6. Audit Records:

The audit log contains information such as the date and time of record entries and updates, system inquiries, etc.

Disposition: DELETE/DESTROY when 25 years old.

7. Backups:

Backups are maintained for potential system/server restoration in the event of a system/server failure or other unintentional loss of data.

Disposition: DELETE/DESTROY/OVERWRITE incremental backup media when superseded by a full backup or when 90 days old.

Disposition: DELETE/DESTROY/OVERWRITE full backup media when one year old.