REQUEST FOR RECORDS DISPOSITION AUTHORITY

REQUEST FOR RECORDS DISPOSITION AUTHORITY	JOB NUMBER *NI-065-07-21*
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001	Date received *9/14/07*

1 FROM (Agency or establishment)

DEPARTMENT OF JUSTICE

2 MAJOR SUBDIVISION

FEDERAL BUREAU OF INVESTIGATION

3 MINOR SUBDIVISION

COUNTERTERRORISM DIVISION

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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10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
Teresa C. Sharkey, CRM	202-324-1613	4/24/08	*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 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,

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

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
9/12/07	*William L. Hooton*	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7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)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 **Counterterrorism (CT) Watch Log System**, which is a system used as a repository for all reported domestic and international threats and suspicious activities		

LO 5/2/08 Copies sent to agency, NR, 9 NWMW

115-109   PREVIOUS EDITION NOT USABLE   **STANDARD FORM 115** (REV 3-91)
Prescribed by NARA 36 CFR 1228

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	Counterterrorism (CT) Watch Log System The Federal Bureau of Investigation's (FBI's) Counterterrorism Division's (CTD's) CT Watch Unit (CTWU) is responsible for the CT Watch Log system. Implemented in 2003, the CT Watch Log system is an Oracle database that is a repository for all reported domestic and international threats and suspicious activities. The FBI Field Offices, Legats, and other government agencies all communicate activities to the CTWU, which operates 24 hours a day, 7 days a week. CTWU logs the information received into the system. Based on the information received, CTWU conducts preliminary analysis, makes immediate assignments for action of threat-related leads, and provides timely alerts to FBI and Department of Justice (DOJ) executives, the White House Situation Room, other government agencies, legal attaches, and field offices and Joint Terrorism Task Forces (JTTF). All of the information received and communications sent out are entered into the CT Watch Log. All of the information in the system has some intelligence or investigative value. Information in the system is sensitive but unclassified (SBU) A. **INPUTS** CTWU staff members key in data, which is typically derived from telephone calls, but also is based on the review of source documents that contain information regarding potential threats and ongoing investigative responses to incidents 1. **Source Records** The primary sources of records are e-mail messages that contain content that is cut and pasted into the system. Other source documents include faxes, teletypes and forms that are reviewed and relevant data is keyed into the system DISPOSITION Delete/Destroy upon successful input into CT Watch Log See Also "CT Watch Back-Up Document Files" (E item 4) 2. **Data Keyed into CT Watch Log** The keyed in data includes, but is not limited to the information (limited to 3,000 characters per record), who sent the information, how the information was received, the actions taken to disseminate the information, the date the action was taken, and the person responsible for handling the action DISPOSITION See "B Data Files"		

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	B. DATA FILES Data files include information input into the system, as described in "Data Keyed into CT Watch Log" (A item 2) and any related metadata DISPOSITION Data File Cut-off at the end of the calendar year Delete/Destroy ten years after Data File Cut-off **C. OUTPUTS** The system does not have the ability to generate reports, but information can be printed out via text files created through searches within the CT Watch Log for relevant data **Text Files** This information includes text files that are printed and filed within the related case file DISPOSITION Retain/Destroy commensurate with the retention periods approved for the file classification in which the case file was opened **D. DOCUMENTATION** These records include system specifications, file specifications, codebooks, user guides, and output specifications 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 later. **E. RELATED RECORDS** 1. **CT Watch Transition Log** These records include information and special instructions used to assist in the CT Watch Unit's daily, three-shift transitions The information is prepared by the staff at the end of their current shift to let the next shift know the actions that have occurred and any action items that need to be completed a. **Transition Log (Original)** These records include the record copy of the transition log that contains the transition staff's initials DISPOSITION File Cut-off at the end of the calendar year Delete/Destroy three years after File Cut-off		

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	b. Transition Log (Distributed Staff Copies) These copies are provided to staff at the time of transition DISPOSITION Delete/Destroy upon completed shift or when no longer of reference value, whichever is later **2. Daily Briefing Book (DBB) Records** **a. CT Watch Commander's DBBs** These books are the CT Watch Commander's copy that is retained in hard copy and/or on CD The books are used as a reference copy DISPOSITION Delete/Destroy when no longer of reference value **b. Daily Briefing Book (DBB), CT Watch's Input** These records include the CT Watch's input into the Director's Briefing Book (DBB) DISPOSITION: Delete/Destroy five years after submission (N1-065-05-4, Item 6) **3. Executive Summaries** These files include incident synopsis created for executives DISPOSITION File Cut-Off at the end of the calendar year Delete/Destroy 10 years after file cut-off		

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	4. CT Watch Back-Up Document Files **a. Hard Copy, 2003-2005** These files have varying contents including a copy of the Transition Log, a copy of related e-mails, and any other related forms and records DISPOSITION File Cut-off at the end of the calendar year Delete/Destroy immediately **b. Electronic Files** These files contain scanned images of varying contents including a copy of the Transition Log, a copy of related e-mails, and any other related forms and records DISPOSITION File Cut-off end of calendar year Delete/Destroy one year after file cut-off **5. CT Watch Daily E-Mail Update, 2003-2005** These files were a snapshot of terrorist related threats and incidents, occurring both domestically and internationally The information was compiled from the CT Watch Logs The information was emailed to select individuals, including the Joint Terrorism Task Forces (JTTF) Coordinator, FBI personnel (e g Legats, etc) who are involved in Counterterrorism (Note the CT Watch Daily E-Mail Update is no longer produced) DISPOSITION File Cut-off at the end of each calendar year Delete/Destroy immediately **6. System Backup Files** Backup tapes 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 **7. Security Audit Logs** These files contain audits related to database-specific events, including logins, accesses, and administrative activities DISPOSITION Delete/Destroy when four (4) years old or when no longer needed for administrative, legal, audit, or other operational purposes, whichever is later		