

REQUEST FOR RECORDS DISPOSITION AUTHORITY		JOB NUMBER N1-566-10-04	
To NATIONAL ARCHIVES and RECORDS ADMINISTRATION 8601 Adelphi Road, College Park, MD 20740-6001		DATE RECEIVED 9/27/10	
1 FROM (Agency or establishment) Department of Homeland Security		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disposition request, including amendments, is approved except for items that may be marked disposition not approved or withdrawn in column 10	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 U S Citizenship and Immigration Services (USCIS)			
3 MINOR SUBDIVISION Verification Division			
4 NAME OF PERSON WITH WHOM TO CONFER Barbara Walker	5 TELEPHONE 202-443-0177	DATE 9/23/10	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 __ page(s) are not needed now 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, <input checked="" type="checkbox"/> is not required, <input type="checkbox"/> is attached, or <input type="checkbox"/> has been requested			
DATE 09/21/2010	SIGNATURE OF AGENCY REPRESENTATIVE Tricia Canard		TITLE USCIS Records Officer
7 Item No	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
1.	<p>Compliance Tracking and Management System (CTMS)</p> <p>CTMS is the compliance tracking and management system for monitoring and compliance activities that support the Verification Division's mission critical function of minimizing misuse, abuse, discrimination, breach of privacy, and fraudulent use of the Systematic Alien Verification for Entitlements (SAVE) and E-Verify programs. The basic capabilities of CTMS include monitoring and compliance activity tracking, data and document collection and storage, incident management tracking and incident history searching, reporting, and workflow management.</p> <p>Applicability: CTMS will be used by Verification Division staff in both Headquarters and Field locations.</p> <p>Specific Restrictions: Access to CTMS is protected from unauthorized users through appropriate administrative, physical, and technical safeguards. The safeguards include restricting access to those with a need to perform their official duty and designating user roles.</p> <p>Vital Records: No</p>		

a. INPUTS

~~Data is scanned, uploaded, and/or typed into CTMS from sources such as~~

- ~~• The Verification Information System (VIS);~~
- ~~• Information from the Verification Call Center, law enforcement agencies, public media, and public data sources that may have bearing on potential cases of misuse, abuse, discrimination, breach of privacy, and fraudulent use of Verification;~~
- ~~• Information from SAVE and E-Verify program users and individuals subject to immigration status verification or employment authorization verification~~

~~DISPOSITION Temporary Delete/destroy when data has been entered into the Master File and verified (Note Source documents are normally copies, not originals. If originals are inadvertently received, they must be returned to the sender or retained in accordance with the applicable schedule.)~~

GRS 20,
Item 2 (4)

b. MASTER FILE

Categories of records in this system include

- Company name, and contact and registration information,
- Agency name, and contact and registration information,
- Individual's name,
- Birth information,
- Citizenship and nationality information,
- Immigrant/non-immigrant information maintained by DHS or Department of State, such as arrival and departure information,
- Identification information such Social Security Number, A-Number, passport and visa information,
- Verification subject contact information such as phone numbers, email addresses, physical addresses,
- SAVE and E-Verify user contact information such as phone numbers, email addresses, physical addresses,
- Analytic information derived from monitoring VIS that may indicate further compliance activities are warranted (this may include any data element contained in VIS),
- Complaint and lead information from VIS redress requests, media reports, and call center compliant reports,
- Information collected during compliance activities including, but not limited to SAVE and E-Verify created documents such as Tentative Non-Confirmation (TNC), referral or compliance letters, Form I-9 and supporting documents, employment offer and termination letters, benefit and credential applications and supporting documents, SAVE and E-Verify user interviews,
- CTMS user information, and
- Status and workflow tracking information

DISPOSITION Temporary Destroy/delete ten (10) years after final action

	<p>c. <u>OUTPUTS</u></p> <p>Standard or ad hoc reports relating to CTMS operations. Users and management can generate reports related to monitoring and compliance operations (such as number of incidents logged per month) as well as specific cases (incidents for a particular employer, contact information, etc.) Reports can be regenerated as needed.</p> <p>DISPOSITION—Temporary—Destroy/delete when no longer needed for administrative, legal, audit, or other agency business.</p> <p>d. <u>SYSTEM DOCUMENTATION</u></p> <p>The following documentation exists for CTMS. System Development Life Cycle (SDLC) documents, including systems specifications, file specifications, data layout documentation, and user guide.</p> <p>DISPOSITION—Temporary—Destroy/delete when system is superseded or when no longer needed for reference purposes.</p>	GRS 20, Item 16	
		GRS 20, Item 11 α,	(i)