REQUEST FOR RECORDS DISPOSITION AUTHORITY

JOB NUMBER *NI-566-05-1*

To: NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR)
WASHINGTON, DC 20408

DATE RECEIVED
9/23-05

1. FROM (Agency or establishment)	NOTIFICATION TO AGENCY
Department of Homeland Security	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disposition request, including amendments, is approved except for items that may be marked disposition not approved or withdrawn in column 10.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

United States Citizenship and Immigration Service (USCIS)

3. MINOR SUBDIVISION

Fraud Detection and National Security

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE	DATE	ARCHIVIST OF THE UNITED STATES
Brenda Ford	(202) 616-1205	*2/16/06*	*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 ____ page(s) are not now needed 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,

[X] is not required; [ ] is attached; or [ ] has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
9/1/05	*Marian L Smith*	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 GRS OR SUPERSEDED JOB CITATION	10.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.	**FRAUD DETECTION AND NATIONAL SECURITY (FDNS) DATA SYSTEM** **Description.** The Fraud Detection and National Security (FDNS) Data System is a case management system that is used to track and control fraud administrative inquiries, criminal referrals, and national security cases. The system will be located at the Vermont Service Center, St. Albans, VT, and will be accessible via the intranet by authorized users. **Categories of Individuals Covered By The System:** Individuals covered by provisions of the Immigration and Nationality Act of the United States (e.g. applicants for immigration benefits), including subjects of administrative inquiries (e.g. applicants, preparers, and representatives) into potentially fraudulent applications for immigration benefits, individuals whose applications have been randomly selected for assessment of the effectiveness of fraud detection programs, and individuals of concern based on possible national security reasons or criminal activity.	*cc NR, NWMD, NWME NWMW, agency*	

The FDNS Data System will interface with all USCIS benefit application data.

Program: Office of Fraud Detection and National Security

Applicability: Agency-wide

Specific Restrictions: Highly sensitive tracking and monitoring information. All records and FDNS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. The safeguards include restricting access to those with a need-to-know to perform their official duties, using a permanent ID and password.

Vital Record: Yes.

Specific Legal Requirements: 8 USC §§ 1103.

Superseded by:

DAA-GRS-2017-0003-0002
DATE (MM/DD/YYYY):
07/2017

a. INPUTS.

Categories of Records In The System:
The FDNS Data System will contain information collected in the process of conducting administrative inquiries (i.e., the process by which USCIS determines if fraud exists) and performing background checks and requests for assistance from law enforcement agencies, including biographical information and corporate information. These records will also include data compiled from the internet and commercial and other governmental data sources such as Choicepoint/Autotrack, Lexis/Nexis, various local, county and state police information networks, various state motor vehicle administration databases, State websites, Driver License retrieval sites, State Bar Associations, CIA Department of State, FAA websites, FedEx tracking, various state comptrollers, appraisal districts (counties), state probation/paroles, American Immigration Lawyers Association, Legal Information Institute, university websites, state sexual predator websites, news media websites, various search engines (e.g. Ask Reeves, Google etc.), Desk Ref, UPI, Reuters, and foreign news media websites.

TEMPORARY. Destroy or delete after the data has been transferred to the masterfile and verified.

Superseded by:

N1-566-08-018
DATE (MM/DD/YYYY):
11/31/2008

b. MASTER FILE.

Types of data elements include:

Fraud Detection and National Security Data Fields					
Case Num	DHS Assoc Number	DHS ICE LEAC Notified Flag	DHS Results	HLSFileDockReqFlg	Source Last Name
Activity UID	DHS Attachment	DHS Interviews	DHS SCClaims	HLSFileSize	Source Organization
BFU Case Number	DHS Birth Date	DHS Last Name	DHS SEVIS	HLSFileSrcType	Source Type
Case	DHS Call Up Date	DHS Level of Investigation	DHS Site Check	Last Name	State
Case Id	DHS Checks	DHS Maiden Name	DHS Source	Middle Name	Status
Case Num	DHS CIS	DHS NAILS	DHS SSN	Name	Synopsis
Case Rel Type Code	DHS City	DHS Nails Number	DHS State	Note	Threat
Citizenship	DHS Class Preference	DHS NIIS	DHS State Motor Vehicles Record	Note Type	Type
City	DHS Closed	DHS Number of Files	DHS State Wage and Earnings Records	Owned By	
Comment	DHS Closed Remarks	DHS Number Reviewed	DHS Status Date	Owned By Id	
Contact Last Name	DHS Confirmed Fraud	DHS Office Code	DHS Street Address	Party Type Code	
Date Created	DHS Contacted Flag	DHS Other	DHS Street Address 2	Place of Birth	
Date Declined BFU	DHS Country	DHS Other Comments	DHS Synopsis	Planned	
Date Occurred	DHS DACS	DHS Owner Fax Number	DHS Tecs	Planned Completion	
Date of Birth	DHS Date of Incident	DHS Owner Phone Number	DHS Text	Position	

Date to BFU	DHS Date of Report	DHS Postal Code	DHS To	Postal Code	
Description	DHS Disposition	DHS Primary Employee Id	DHS To Title	Priority	
DHS A Number	DHS Distribution	DHS Primary Phone #	Due	Private	
DHS Activity Type	DHS Division	DHS Public Record Information	End Date	Reason Declined BFU	
DHS Adjudications	DHS Division Id	DHS RAPS	First Name	SAC Office	
DHS Admin Inquiry	DHS Enclosures	DHS Receipt Number	HLS Created	Sales Rep	
DHS Alias First Name	DHS Files	DHS Recommendation Action	HLS Created By	Short Comment	
DHS Approved By	DHS First Name	DHS Recommendations	HLS Created By Name	Source	
DHS Approved Date	DHS Fraud Results	DHS Record of Action Taken	HLSFileAutoUpdFlg	Source First Name	
DHS Approving IO	DHS IBIS	DHS Reliability	HLSFileDate	Source Id	

TEMPORARY. Delete/Destroy when 75 years old. If the data becomes too large it will be copied onto electronic media and stored at the Department of Justice Data Center in Rockville, MD or Dallas, TX.

Note: DHS/BICE agrees to maintain these records in accordance with 36 CFR 1234 §§ 30-32 for their entire 75-year retention period.

c. **OUTPUTS:** Reports, etc.

    TEMPORARY. Delete/destroy when no longer needed for agency business.

d. **System Documentation:**

    User Manual

    TEMPORARY. Destroy when the system becomes obsolete, superseded, or no longer needed for agency business.

Superseded by:

DAA-6RS-2017-0003-001
DATE (MM/DD/YYYY):
07/2017

Superseded by:

DAA-6RS-2013-0005-0003
DATE (MM/DD/YYYY):
01/2017

Privacy Act Restriction: 552a (b) (3) The Secretary of Homeland Security has exempted this system from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5) and (8) and (g) of the Privacy Act. These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). The Department of Homeland Security has published implementing regulations in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and these have been published in the Federal Register and can be found at 6 CFR Appendix C to Part 5.