Amount of Award: Remainder of current budget period February 1, 2009, through September 29, 2009; Award is $286,458. Final budget period of the originally approved five-year project period through September 29, 2010; Annual Amount $300,000.

Projected Period: February 1, 2009–September 29, 2010.

SUMMARY: In FY 2005, ORR awarded a competitive service grant for the Individual Development Account (IDA) Program grant to New York Association for New Americans, Inc. (NYANA) in New York, NY. The original project was from September 29, 2005, through September 30, 2010. NYANA served as the fiscal sponsor and legal entity of the approved project. As of February 1, 2009, NYANA has ceased operations of the Individual Development Account program. NYANA has requested ORR permission for the Center for Community Development for New Americans (CCDNA) to assume the grant. CCDNA has agreed to this request. The effect of this deviation request is to transfer the grant from the initial grantee to a new grantee with all the responsibilities of managing and implementing the project for the remainder of the grant period.

Contact Information: Ronald Munia, Director, Division of Community Resettlement, Office of Refugee Resettlement, 370 L'Enfant Promenade, SW., Washington, DC 20447. Telephone (202) 401–4559. E-mail: *Ronald.munia@acf.hhs.gov*.

Dated: April 30, 2009.

Ronald Munia,

Director, Division of Community Resettlement, Office of Refugee Resettlement.

[FR Doc. E9–11961 Filed 5–21–09; 8:45 am]

BILLING CODE P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2009–N–0664]

Food and Drug Administration Clinical Trial Requirements; Public Workshop

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of public workshop.

SUMMARY: The Food and Drug Administration (FDA) Minneapolis District, in cosponsorship with the Society of Clinical Research Associates, Inc. (SoCRA) is announcing a public workshop entitled ''FDA Clinical Trial Requirements.'' This 2-day public workshop is intended to provide information about FDA clinical trial requirements to the regulated industry.

Date and Time: The public workshop will be held on Wednesday, June 10, 2009, from 8:30 a.m. to 5 p.m., and Thursday, June 11, 2009, from 8:30 a.m. to 5 p.m.

Location: The public workshop will be held at the Radisson University Hotel, Suite 600, 615 Washington Ave., SE., Minneapolis, MN 55414, 612–379–8888 or 1–800–822–6757 or 888–201–1718.

Contact: Carrie Hoffman, Food and Drug Administration, 250 Marquette Ave., Minneapolis, MN 55401, 612–758–7200, FAX: 612–334–4142, e-mail: *carrie.hoffman@fda.hhs.gov*.

Attendees are responsible for their own accommodations. To make reservations at the Radisson University Hotel, contact the Radisson University Hotel (see *Location*).

Registration: You are encouraged to register by June 9, 2009. The SoCRA registration fees cover the cost of facilities, materials, and breaks. Seats are limited; please submit your registration as soon as possible. Course space will be filled in order of receipt of registration. Those accepted into the course will receive confirmation. Registration will close after the course is filled. Registration at the site is not guaranteed but may be possible on a space available basis on the day of the public workshop beginning at 8 a.m. The cost of registration is as follows: FDA employee (fee waived), Government employee nonmember ($525), non-Government employee SoCRA member ($575), non-Government employee non-SoCRA member ($650).

If you need special accommodations due to a disability, please contact Carrie Hoffman (see *Contact*) at least 7 days in advance of the workshop.

Registration Instructions: To register, please submit a registration form with your name, affiliation, mailing address, phone, fax number, and e-mail, along with a check or money order payable to ''SoCRA.'' Mail to: SoCRA, 530 West Butler Ave., Suite 109, Chalfont, PA 18914. To register via the Internet, go to *http://www.socra.org/html/FDA_Conference.htm.* (FDA has verified the Web site address, but we are not responsible for any subsequent changes to the Web site after this document publishes in the **Federal Register.**)

The registrar will also accept payment by major credit cards (VISA/MasterCard/AMEX only). For more information on the meeting, or for questions on registration, contact SoCRA at 800–762–7292 or 215–822–8644, FAX: 215–822–8633, or e-mail: *SoCRAmail@aol.com.*

SUPPLEMENTARY INFORMATION: The public workshop helps fulfill the Department of Health and Human Services' and FDA's important mission to protect the public health. Topics for discussion include the following: (1) What FDA Expects in a Pharmaceutical Clinical Trial; (2) Adverse Event Reporting—Science, Regulation, Error and Safety; (3) Part 11 Compliance—Electronic Signatures; (4) Informed Consent Regulations; (5) IRB Regulations and FDA Inspections; (6) Keeping Informed and Working Together; (7) FDA Conduct of Clinical Investigator Inspections; (8) Meetings with FDA: Why, When, and How; (9) Investigator Initiated Research; (10) Medical Device Aspects of Clinical Research; (11) Working with FDA's Center for Biologics Evaluation and Research; (12) The Inspection is Over—What Happens Next? Possible FDA Compliance Actions.

FDA has made education of the drug and device manufacturing community a high priority to help ensure the quality of FDA-regulated drugs and devices. The workshop helps to achieve objectives set forth in section 406 of the FDA Modernization Act of 1997 (21 U.S.C. 393) which includes working closely with stakeholders and maximizing the availability and clarity of information to stakeholders and the public. The workshop also is consistent with the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), as outreach activities by Government agencies to small businesses.

Dated: May 18, 2009.

Jeffrey Shuren,

Associate Commissioner for Policy and Planning.

[FR Doc. E9–12051 Filed 5–21–09; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0015]

Privacy Act of 1974; United States Citizenship Immigration Services 009 Compliance Tracking and Monitoring System; System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of

Homeland Security proposes to establish a new Department of Homeland Security system of records notice titled, DHS/USCIS—009 Compliance Tracing and Monitoring System (CTMS). CTMS collects and uses information necessary to support monitoring and compliance activities for researching and managing misuse, abuse, discrimination, breach of privacy, and fraudulent use of USCIS Verification Division's verification programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. This newly established system will be included in the Department of Homeland Security's inventory of records systems.

DATES: Submit comments on or before June 22, 2009. This new system will be effective June 22, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2009–0015 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Claire Stapleton (202–358–7777) Verification Division Privacy Branch Chief, or Donald K. Hawkins (202–272–1400), Citizenship and Immigration Services Privacy Officer, 20 Massachusetts Avenue, NW., Washington, DC 20529, U.S. Citizenship and Immigration Services, Department of Homeland Security, 470 L'Enfant Plaza East, SW., Suite 8204, Washington, DC 20529. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The United States Citizenship and Immigration Services (USCIS) Verification Division supports two congressionally mandated programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify programs. E-Verify, formerly known as the Basic Pilot Program, was established under the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104–208 section 401, 8 U.S.C. 1324a note. SAVE was established under the Immigration and Control Act of 1986, Public Law 100–360 section 121(c). Congress mandated SAVE to provide government agencies with citizenship and immigration status information for use in determining an individual's eligibility for government benefits. The SAVE program allows Federal, State, and local government benefit-granting agencies, as well as licensing bureaus and credentialing organizations to confirm the immigration status of non-citizen applicants, by submitting to SAVE certain information supplied by the benefit applicant. Congress mandated E-Verify for use by employers to determine whether an employee is authorized to work in the United States at the time that he or she begins working. The E-Verify program allows participating employers to verify the employment eligibility of all newly hired employees, by submitting to E-Verify specific information supplied by the employee.

The SAVE and E-Verify programs rely on the Verification Information System (VIS) as the underlying technical infrastructure as described in the Verification Information System SORN, DHS–USCIS–004, December 11, 2008, 73 FR 75445, and VIS Privacy Impact Assessments. As part of the mandate to implement the SAVE and E-Verify programs, Congress imposed various legal and operational requirements including requirements to insulate and protect the privacy and security of collected information, to prevent unauthorized disclosure of personal information, and to have safeguards against the system resulting in unlawful discrimination. In order to ensure that these requirements are met, the Verification Division created the Monitoring and Compliance (M&C) Branch which, as one might imagine, will be responsible for two distinct set of tasks: monitoring and compliance. M&C will monitor the verification transactions within VIS to identify potential cases of misuse, abuse, discrimination, breach of privacy, or fraudulent use of SAVE and E-Verify. When M&C identifies certain defined anomalous activities through these monitoring efforts they may take additional compliance steps to verify and correct these activities. These activities are referred to as noncompliant behaviors.

The M&C Branch is developing detailed procedures for both monitoring the verification transactions in VIS and for performing compliance activities on defined non-compliant behaviors. For example, one type of behavior is associated with the misuse of SSN. For this behavior M&C will identify when a single social security number is used multiple times for employment authorization verifications through E-Verify. It would not be uncommon for a single individual to be verified several times through E-Verify as one person may hold multiple jobs or change jobs frequently, but it would be unusual for a single individual to hold 30 or 40 jobs simultaneously. M&C has developed procedures for identifying when a certain threshold number of verifications of a single SSN would be likely to indicate some type of misuse. If this threshold is met then M&C would conduct certain specific compliance activities that may involve collecting or looking at information from outside of VIS. This might include contacting or visiting an employer to research the issue and determine if there is: a system problem which the Verification Division needs to correct; if there is a user misunderstanding which requires additional training for the employer, or potentially fraudulent activity which may need to be reported to law enforcement agency.

In most cases compliance activities will be undertaken based on monitoring defined behaviors in VIS. However, there are some behaviors which may not necessarily be indicated by monitoring VIS. For example, employers are required to conspicuously post notification of their participation in E-Verify to their employees. This notification provides the employees with information concerning their rights and responsibilities regarding E-Verify, including contact information. Obviously there is no information in VIS that would indicate whether an employer had actually posted these notices. Compliance activities around the non-compliant behavior of failing to post the required notices would most likely occur based on a complaint/hotline report or during a compliance visit researching another potential behavior. M&C might also identify potential non-compliant behaviors from media reports or tips for law enforcement agencies.

The management of compliance activities and storage of the supporting information will be handled by the Compliance Tracking and Management System (CTMS). 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.

CTMS will be developed in increments. Initially, it will be based on existing and new consumer-off-the-shelf (COTS) technology products required to meet basic capabilities. This includes database and analysis technologies that are currently available in the Verification Division, and new data storage and business process workflow systems. It is anticipated that CTMS will also grow to include additional and more sophisticated analytic and information management functionality. As the system develops, USCIS will update the SORN and PIA as appropriate.

Initially, CTMS will be used to support a range of monitoring and compliance activities, which include researching and documenting the following non-compliant agency or employer categories of behaviors:

- Fraudulent use of Alien-Numbers (A-Numbers) and SSNs by E-Verify users;
- Termination of an employee because he receives a tentative non-confirmation (TNC) [1];
- Failure of an employer to notify DHS, as required by law, when an employee who receives a final non-confirmation (FNC) is not terminated;
- Verification of existing employees (as opposed to new hires);
- Verification of job applicants, rather than new employees (pre-screening);
- Selectively using E-Verify or SAVE for verifications based on foreign appearance, race/ethnicity, or citizenship status;
- Failure to post the notice informing employees of participation in E-Verify;
- Failure to use the E-Verify, consistently or at all, once registered;
- Failure of SAVE agency to initiate additional verification when necessary;
- Unauthorized searching and use of information by a SAVE agency user; and
- Fraudulent use of visas, permits, and other DHS documents by SAVE users.

[1] A tentative non-confirmation (TNC) occurs when E-Verify is unable to match the information provided by the employer with the information in DHS records. Employees can choose to contest the TNC by contacting either SSA or DHS and following the established procedures.

Monitoring

Generally speaking these categories of behaviors, as described more fully below, will usually be identified by monitoring the information in VIS. They may also be identified based on tips received from affected individuals, various law enforcement agencies, or the media. They may be the result of a Privacy Act redress request. With regard to the behavior of failing to post appropriate notice, it could be identified during a compliance visit to an employer for research on another potential non-compliant behavior. As noted above, monitoring for behaviors is complicated by the fact that not all anomalous transactions in VIS will necessarily indicate a non-compliant behavior. Thus M&C is establishing thresholds to narrow their research to find the most likely cases of non-compliant behaviors. Once M&C has established there is likely an occurrence of a non-compliant behavior M&C will extract the minimal amount of data necessary to identify possible non-compliant behavior. The minimal amount of data necessary is only data that is directly related to making a determination about the alleged non-compliant behavior. That data is entered into CTMS to conduct compliance activities.

Compliance

Compliance activities are meant to stop misuse, abuse, discrimination, breach of privacy, and fraudulent use of SAVE and E-Verify. These activities could result in a range of outcomes including correcting a SAVE or E-Verify system problem, providing additional SAVE and E-Verify user training or assistance to ensure correct use of these systems, turning off access to SAVE and E-Verify for individual users who continue to misuse the systems, or contacting law enforcement agencies in the case of suspected illegal activities.

Once the monitoring analyst determines a behavior meets the threshold the compliance analyst may begin researching the behavior. The specific research will vary depending on the behavior but generally could involve contacting or visiting the SAVE or E-Verify user (a government agency or employer respectively), to notify them that they may not be in compliance with program requirements. This notification will allow the SAVE and E-Verify user to remediate or explain the issue. In some cases, if the program user is unable to remediate or explain the issue, additional research may be conducted, including collecting supporting information from other sources beyond VIS. This may include the collection of such information as E-Verify or SAVE created documents (such as an E-Verify Tentative Non-Confirmation (TNC) letter or referral letters), Forms I–9 and copies of supporting documents, employment offer or termination letters, information collected during interviews with SAVE and E-Verify users [2] related to program participation.

M&C efforts are focused on misuse of the E-Verify and SAVE program. M&C will concentrate compliance operations, such as interviews or document requests, directly on the users of these systems—the employers or government agencies, rather than on the individuals who are verified. M&C would only contact a SAVE or E-Verify subject directly when a compliance activity is based on a redress request or hotline tip. When appropriate, interviews will be conducted in a confidential manner. Information received during interviews and complaints will be kept confidential unless required to be released based on legal necessity. If a particular behavior is substantiated, the Verification Division will take appropriate steps to correct this behavior including requiring additional training, restricting access to SAVE or E-Verify, or referral to a law enforcement agency for further action. Concurrently with the publication of this SORN, the Verification Division is publishing a notice of proposed rulemaking to pursuant to 5 U.S.C. 552a(k)(2), to exempt CTMS from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(4)(G), and (e)(4)(H).

Information in CTMS is used to prevent misuse and illegal activities. Consequently, this SORN has a routine use for sharing with Federal, State, local, and Tribal law enforcement agencies, as well as for other standard DHS routine uses.

Consistent with DHS's information sharing mission, information stored in CTMS may be shared with other DHS components, as well as appropriate Federal, State, local, Tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to

[2] An E-Verify user is anyone in a company/agency enrolled with E-Verify, who actually uses E-Verify to verify other individuals, or others who have a relationship/association with E-Verify such as a designated point of contact or Memorandum of Understanding (MOU) signatory. Similarly, SAVE users are deemed to be individuals who actually use SAVE to verify other individuals, or others who have a relationship/association with SAVE. Users do not include individuals who have no relationship with SAVE or E-Verify except that they may have been verified through these programs.

know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the USCIS, Verification Division, DHS/USCIS—009 Compliance Tracking and Monitoring System of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

DHS/USCIS–009

SYSTEM NAME:

DHS/USCIS–009 Compliance Tracking and Monitoring System.

SECURITY CLASSIFICATION:

Sensitive but unclassified.

SYSTEM LOCATION:

Records are maintained at USCIS Headquarters in Washington, DC, in USCIS field offices, and at a contractor-owned facility in Meriden, CT. The system is accessible in a secure manner to authorized USCIS personnel via the Internet.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains information on four categories of individuals, any of whom may be either U.S. citizens or non-U.S. citizens. These include:

1. *Verification Subjects:* Individuals who are the subject of E-Verify or SAVE verifications and whose employer is subject to compliance activities,

2. *E-Verify or Save Program Users:* Individuals who use, are enrolled users, or have an agency or employment responsibility associated with the SAVE or E-Verify programs,

3. *Complainants:* Individuals who have contacted the Verification Division or publicly reported potential cases of misuse, abuse, discrimination, breach of privacy, and fraudulent use of USCIS Verification Division's verification programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify, and

4. *DHS Employees:* Verification Division employees or contractors who are involved in SAVE and E-Verify monitoring and compliance activities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's name;
- Verification Subjects birth information;
- Verification Subjects citizenship and nationality information;
- Verification Subjects immigrant/non-immigrant information maintained by DHS or Department of State, such as arrival and departure information;
- Verification Subjects identification information such Social Security Number, A-Number, passport and visa information;
- Verification Subjects contact information such as phone numbers, e-mail addresses, physical addresses;
- SAVE and E-Verify user contact information such as phone numbers, e-mail 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 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; and
- CTMS user information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The authority for the maintenance of records in the system is found in 8 U.S.C. 1324a, 8 U.S.C. 1360, 42 U.S.C. 1320b-7 and the Immigration Reform and Control Act of 1986 (IRCA), Public Law (Pub. L.) 99–603, The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA), Public Law 104–193, 110 Stat. 2168, Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, 110 Stat. 3009, 18 U.S.C. 3291, and in Executive Order 12989, as amended by Executive Order 13465, June 6, 2008.

PURPOSE(S):

The purpose of this system is to analyze, collect, and manage information necessary to support monitoring and compliance activities for researching and managing misuse, abuse, discrimination, breach of privacy, and fraudulent use of USCIS Verification Division's verification programs, the Systematic Alien Verification for Entitlements (SAVE) and E-Verify.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3).

Routine uses include disclosure to:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, Tribal, or local law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the DOJ, Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or nationality discrimination.

I. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

This is an analytic and data management system that allows for retrievability on any data element collected. For example, records may be retrieved by a name or other unique identifiers to include: verification number, A-Number, I–94 Number, Visa Number, SSN, or by the submitting employer or agency name.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

The following proposal for retention and disposal is being prepared to be sent to the National Archives and Records Administration for approval. Records collected in the process of establishing immigration and citizenship status or employment authorization are stored and retained in the VIS Repository for ten (10) years from the date of the completion of the verification unless the records are part of an on-going investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possible using VIS (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents).

SYSTEM MANAGER AND ADDRESS:

Chief, Verification Division, U.S. Citizenship and Immigration Services, 470–490 L'Enfant Plaza East, SW., Suite 8206, Washington, DC 20529.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, USCIS, Verification Division will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the headquarters or component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Lane, SW., Building 410, Mail STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records come from several sources including: (1) Information from VIS reflecting the monitoring analysis of VIS systems users, potentially including any data fields that are allowed for VIS under the current VIS SORN, 73 FR 75445; (2) complaints, questions, and tips from SAVE and E-Verify users and individuals subject to immigration status verification provided by callers to the Verification Call Center; (3) information collected on potential cases of misuse, abuse, discrimination, breach of privacy, and fraudulent use of Verification programs from various media or law enforcement organizations to include media leads or external requests; and (4) information collected from compliance reviews undertaken by the M&C staff which have been provided by the E-Verify employer or SAVE user regarding the compliance review, which may include, but is not limited to: Form I–9 and supporting documents; benefit or credential applications and supporting documents: government documents such as SSNs, visas, DHS and Department of State issued benefit documents, and passports; employment offer and termination letters; and notes of interviews.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security plans to claim an exemption for this system from 5 U.S.C. 552a (c)(3), (d), (e)(4)(G), and (e)(4)(H) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

Dated: May 15, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–11967 Filed 5–21–09; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

United States Immigration and Customs Enforcement

[OMB Control No. 1653–0037]

Agency Information Collection Activities: Extension of an Existing Information Collection; Comment Request

ACTION: 60-day notice of information collection for review; notice to student or exchange visitor.

The Department of Homeland Security, U.S. Immigration and Customs Enforcement (USICE), will be submitted the following information collection request for review and clearance in accordance with the Paperwork Reduction Act of 1995. The information collection is published to obtain comments from the public and affected agencies. Comments are encouraged and will be accepted for sixty days until July 21, 2009.

Written comments and suggestions regarding items contained in this notice, and especially with regard to the estimated public burden and associated response time, should be directed to the Department of Homeland Security (DHS), Joseph M. Gerhart, Chief, Records Management Branch, U.S. Immigration and Customs Enforcement, 500 12th Street, SW., Room 3138, Washington, DC 20024; (202) 732–6337.

Comments are encouraged and will be accepted for sixty days until July 21, 2009. Written comments and suggestions from the public and affected agencies concerning the proposed collection of information should address one or more of the following four points:

(1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agencies estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses.

Overview of this information collection:

(1) *Type of Information Collection:* Extension of currently approved information collection.

(2) *Title of the Form/Collection:* Notice to Student or Exchange Visitor.

(3) *Agency Form Number, if any, and the Applicable Component of the Department of Homeland Security Sponsoring the Collection:* I–515A, U.S. Immigration and Customs Enforcement.

Affected Public Who Will Be Asked or Required to Respond, as Well as a Brief Abstract: Primary: Individuals or Households. When an academic student (F–1), vocational student (M–1), exchange visitor (J–1), or dependent (F–2, M–2 or J–2) is admitted to the United States as a nonimmigrant alien under section 101(a)(15) of the Immigration and Nationality Act (Act), he or she is required to have certain documentation. If the student or exchange visitor or dependent is missing documentation, he or she is provided with the Form I–515A, Notice to Student or Exchange Visitor. The Form I–515A provides a list of the documentation the student or exchange visitor or dependent will need to provide to the Department of Homeland Security (DHS), Student and Exchange Visitor Program (SEVP) office within 30 days of admission.

(5) *An Estimate of the Total Number of Respondents and the Amount of Time Estimated for an Average Respondent to Respond:* 8,000 responses at 10 minutes (0.1667 hours) per response.

(6) *An Estimate of the Total Public Burden (In Hours) Associated with the Collection:* 1,333.6 annual burden hours

Requests for a copy of the proposed information collection instrument, with instructions; or inquiries for additional information should be requested via e-mail to: *forms.ice@dhs.gov* with ''ICE Form I–515A'' in the subject line.