not exceed 162 and groups will last approximately 90 minutes.

• Case Study Key Informant Interviews (7 versions). The Case Study Key Informant Interviews (CSIs) include 7 qualitative interview versions: (1) Administrator, (2) Counseling Staff, (3) Coalition Member—Faculty, (4) Prevention Staff, (5) Case Finder, (6) Campus Police, and (7) Student Leader. Local project staff will be responsible for identifying appropriate respondents for each CSI version and scheduling the interview to occur during site visits by the case study team. A total of 16 interviews will be conducted during each campus site visit (a total of up to 192 interviews). The case study team from Macro International Inc. will be responsible for administering the interviews and is trained in qualitative interviewing. Sixteen individuals from each of the campus sites will be selected as key informants to participate in the CSIs in the first and third stages of the GLS Campus Case Studies, for a total of 64 respondents. Questions on the CSIs include whether respondents are aware of suicide prevention activities, what the campus culture is related to suicide prevention, and what specific efforts are in place to prevent suicide among the campus population. Items are formatted as open-ended and semi-structured questions. The CSIs include 16 to 21 items and will take approximately 60 minutes to complete. On the second site visit, the case study team will incorporate preliminary findings from the case studies in the interviews, which may be modified to some extent to collect more comprehensive information and gather feedback from local key informants surrounding the context of the preliminary findings. The CSIs for the second site visit will last 60 minutes.

The average annual respondent burden is estimated below. This project is scheduled to be completed in 12 months; thus, the table reflects the total burden for one year, the project length. The estimate reflects the total annual respondents for the project (at which time the CCS would conclude), the average annual number of respondents, the average annual number of responses, the time it will take for each response, and the average burden.

TOTAL AND ANNUAL AVERAGES: RESPONDENTS, RESPONSES AND HOURS

Measure name	Number of respondents	Number of responses per respondent	Hours/response	Response burden
Enhanced Module	1200	1	0.17	204
Focus Group—Student Version	324	1	1.5	486
Focus Group—Faculty Version	108	1	1.5	162
Focus Group—Staff Version	54	1	1.5	81
Interview—Student Leader Version	12	1	1	12
Interview—Case Finder Version	6	1	1	6
Interview—Faculty Version	12	1	1	12
Interview—Campus Police Version	12	1	1	12
Interview—Counseling Staff Version	12	1	1	12
Interview—Prevention Staff Version	18	1	1	18
Interview—Administrator Version	12	1	1	12
Total	590	.....	.....	1317

Send comments to Summer King, SAMHSA Reports Clearance Officer, Room 7–1044, One Choke Cherry Road, Rockville, MD 20857 and e-mail her a copy at *summer.king@samhsa.hhs.gov*. Written comments should be received within 60 days of this notice.

Dated: August 11, 2008.

Elaine Parry,

Acting Director, Office of Program Services.

[FR Doc. E8–19071 Filed 8–15–08; 8:45 am]

BILLING CODE 4162–20–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0072]

Privacy Act of 1974: U.S. Immigration and Customs Enforcement, ICE Pattern Analysis and Information Collection (ICEPIC) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Modification to an existing system of records.

SUMMARY: U.S. Immigration and Customs Enforcement (ICE) is re-publishing the system of records notice (SORN) for the ICE Pattern Analysis and Information Collection (ICEPIC) system to address comments received through the **Federal Register** comment procedure. A minor change has been made to the SORN to update the contact point for individual requests for access to and amendment of records in the system and to propose a new routine use for investigation and remediation of any loss or compromise of personal data from the system, should such a loss or compromise occur.

On January 30, 2008, ICE originally established this system of records and published the SORN and associated proposed rulemaking in the **Federal Register**, 73 FR 5577 and 73 FR 5460 (Jan. 30, 2008). ICE received and considered the public comments, all of which were generally in favor of the system and the proposed rule. In light of the comments received, ICE concluded that no changes to the SORN are warranted at this time other than the proposed addition of a new routine use and to update the contact point for requests to access and correct system records. A final rulemaking is also published in this issue of the **Federal Register** in which the Department exempts portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: The established system of records was effective as of February 29, 2008, based upon the prior ICEPIC system of records notice published on January 30, 2008. Comments are being solicited on the new routine use proposed in this notice. Written comments must be submitted on or before September 17, 2008. The new routine use will be effective September 17, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0072 by one of the following methods:

• *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *Fax:* 1–866–466–5370.

• *Mail:* Hugo Teufel III, 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: Lyn Rahilly, Privacy Officer, (202–514–1900), U.S. Immigration and Customs Enforcement, 425 I Street, NW., Washington, DC 20536, e-mail: *ICEPrivacy@dhs.gov,* or Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Part of ICE's mission is to investigate possible violations of U.S. immigration law. Many times this involves hours of analysis regarding a particular case or operation. As part of the investigative process analysts must identify and understand the relationships among individuals, places, and items that are the subject of investigation.

The ICEPIC Tool builds on earlier ICE initiatives to verify the identity of Special Interest Aliens (SIAs), as designated by the Department of State. In 2003 ICE implemented the National Security Entry Exit Registration System (NSEERS) to manage the growing collection of over 500,000 SIA records. National and international terrorist threats in the 2004 and 2005 timeframe resulted in ICE reviewing not only the SIA records in NSEERS, but also the records of aliens registered with the Student and Exchange Visitor Information System (SEVIS) and entered into the United States Visitor and Immigrant Status Indicator Technology (US VISIT) system as well. Since 2005, ICE's expanding law enforcement role has demanded increasingly sophisticated tools to detect potential violations of immigration and criminal law and terrorist threats.

ICE analyzes relationships among individuals using conventional database queries and link analysis tools; however, traditional link analysis tools rely on the consistency of key data, such as names and addresses, to establish relationships. If the source data is of poor quality or an individual seeks to conceal his/her identity through intentional, but subtle, changes to names, addresses, and other biographic information, then conventional tools are less effective at recognizing relationships. As a result, investigators and analysts may miss important relationships among suspects, family members, other associates, organizations, addresses, and vehicles.

ICEPIC allows ICE law enforcement agents and analysts to look for non-obvious relationship patterns among individuals and organizations that are indicative of violations of the customs and immigration laws that are enforced by DHS agencies, as well as possible terrorist threats and plots. From these relationships, ICE agents can develop specific leads and law enforcement intelligence for active and new investigations. Identified relationships can also be recorded for reuse in subsequent investigative analyses. The information processed by ICEPIC comes from existing ICE investigative and apprehension records systems, as well as immigration and alien admission records systems. All ICEPIC activity is predicated on ongoing and valid law enforcement investigations.

ICEPIC includes capabilities that assist investigators to record results of analyses performed in support of investigations and to capture additional relevant information obtained from outside sources. The information collected by, on behalf of, in support of, or in cooperation with DHS and its components may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies or organizations.

ICEPIC assists ICE investigators by automating five business processes:

A. Analysis of leads, law enforcement and intelligence reports, referrals, and processing of queries of ICE and DHS information to locate relevant records and produce reports;

B. Integration and resolution of information from multiple ICE and DHS databases to provide leads for law enforcement investigations and disruption of potential terrorist activities;

C. Initiation of analyses that support investigative cases in DHS and field offices and recording the results of beneficial analyses;

D. Production and dissemination of target indicator profiles and other law enforcement intelligence; and

E. Management of analysis workflows and information resources.

Information that is produced or maintained by ICEPIC is used by ICE agents in headquarters and field offices to identify potential violations of customs or immigration law, confirm suspected violations, or investigate potential terrorist threats. ICEPIC is used to identify relationships among different individuals or among records for the same individual from multiple sources when an individual or individuals have been identified as subjects, leads, or associates in an investigative case. In cases where DHS determines that the information would assist in the enforcement of civil or criminal laws, ICE may share the information with the appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations. Information may also be used by national intelligence community agencies where analysis of the records indicates a potential or confirmed threat of terrorist activity justifying further analysis or investigation. ICE may also share this information with the FBI when ICE becomes aware of information that may be related to an individual in the Terrorist Screening Database.

The Department of Justice (DOJ) and other Federal agencies may use reports generated through ICEPIC in the review, settlement, and prosecution of claims, complaints, and lawsuits involving matters over which ICE exercises jurisdiction or when conducting litigation or in proceedings before any court, adjudicative, or administrative body. This includes any litigation matters where ICE, DOJ, or an employee in his or her official capacity in support of ICE, the United States, or any agency thereof is involved.

For a more detailed description of the origin and purpose of this system and its functionality, the Privacy Impact Assessment published at *http://www.dhs.gov/privacy* (follow link to ''privacy impact assessments.'').

Because ICEPIC contains information that relates to official DHS national security, law enforcement, immigration, and intelligence activities and is used in support of those activities, the Department published a proposed rulemaking seeking to exempt the ICEPIC system of records from various provisions of the Privacy Act, including the requirement that individuals be provided access to and correction of their own records. These exemptions are permitted by the Privacy Act and are needed to protect information relating to DHS law enforcement or intelligence activities from disclosure to subjects or

others related to these activities. For a complete discussion of the specific exemptions proposed and the reasons they were claimed, please see the notice of proposed rulemaking in the **Federal Register**, 73 FR 5577 (Jan. 30, 2008). A final rulemaking is published concurrently to this notice in this issue of the **Federal Register**.

Public Comments

In the January 30, 2008 publication of the ICEPIC SORN, the Department requested public comments on the SORN and the proposed rulemaking. ICE received and considered the public comments, which are discussed further below, and concluded that no substantive changes to the SORN are warranted at this time. However, ICE is updating the SORN to change the contact information for submission of requests to access and amend records in this system.

Six comments were received. While all comments were in favor of the proposed rule, two commenters also raised specific concerns related to this system of records. Those concerns are addressed below.

One commenter expressed concern that individuals would be unable to ensure their personal information in ICEPIC is accurate unless they are permitted access to their records. Other means exist to verify the accuracy of ICEPIC data and ensure that incorrect data are not used to prejudice that individual. ICEPIC users are trained to verify information obtained from ICEPIC before including it in analytical reports that will be used during investigations or shared with government personnel outside of ICE. Verification procedures include direct queries to the source databases from which ICEPIC originally obtained the information, queries of commercial or other government databases, and ICE agent interviews with individuals or others who are in a position to confirm the ICEPIC data. These procedures mitigate the risk posed by inaccurate data in the system and raise the probability that such data will be identified and corrected before any action is taken that would prejudice an individual. In addition, the source systems from which ICEPIC obtains information may, themselves, have mechanisms in place to ensure the accuracy of the data prior to the information being accessed through ICEPIC.

Another commenter, while in favor of the system, expressed concerns as follows:

''By limiting access to a small number of people, power and responsibility may be monopolized in the hands of some who are never given a system of checks and balances over their power. The only other concern that I have is that, as domestic and international security policies and concerns shift over time, this proposed rule change will be stagnant. I would propose then that this rule be revisited in the coming years as security threats continue to fluctuate.''

To ensure the system contains appropriate checks and balances to oversee those who have access to ICEPIC information, ICE has established appropriate controls and safeguards that provide oversight of authorized ICEPIC users. All user activity is audited and subject to periodic review to identify unauthorized use or activity. ICE investigates instances of unauthorized or inappropriate access or use of the system and takes appropriate disciplinary actions where violations have occurred.

The commenter also recommended a review of this system in the future because ''security threats continue to fluctuate.'' ICE and DHS continue to exercise diligence in the response to the evolving threat environment. Should there be a need to substantially alter this system in the future, similar public notice and an opportunity to comment will be provided.

Proposed Routine Use

ICE is proposing to include a new routine use to support the investigation and remediation of any suspected or confirmed compromise of personal data from the system (*i.e.*, a ''data breach''). This routine use would allow ICE to share information with other agencies, entities, contractors, or individuals for the purpose of supporting ICE's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy any risk of harm. ICE is soliciting comments on this proposed routine use pursuant to 5 U.S.C. 552a(e)(11).

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 personally identifiable information. 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 from which information is retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of the Department by complying with the Department's Privacy Act regulations, 6 CFR part 5.21 and DHS will review each request on a case-by-case basis in light of exemptions taken by ICEPIC.

The Privacy Act requires each agency to publish in the **Federal Register** a description of 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 which personally identifiable information is put, and to assist individuals in finding such files within the agency. In accordance with 5 U.S.C. 552a(r), the Department has provided a report of this revised system of records to the Office of Management and Budget and to the Congress.

SYSTEM OF RECORDS:

DHS–ICE–002.

SYSTEM NAME:

ICE Pattern Analysis and Information Collection.

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

U.S. Department of Homeland Security Immigration and Customs Enforcement Headquarters data facilities are located in the Virginia suburbs of Washington, DC, with continuity of operations sites in remote locations within the continental United States.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Individuals or entities who are associated with investigations, inspections, apprehensions, detentions, patrols, removals, examinations, naturalizations, intelligence production, legal proceedings, or other operations that implement and enforce the Immigration and Nationality Act (INA) (8 U.S.C. 1101 *et seq.*) and related treaties, statutes, orders, and regulations.

B. Individuals or entities who are associated with investigations, inspections, apprehensions, detentions, law enforcement intelligence production, legal proceedings or other operations that implement and enforce immigration- and customs-related laws, specifically those found in Titles 8, 19, and 31 of the United States Code.

C. Individuals who are respondents, representatives, or witnesses in administrative, civil penalty, or forfeiture proceedings, or defendants, representatives or witnesses in criminal prosecution or extradition proceedings

under immigration or customs-related laws or regulations.

D. Associates of the above individuals and entities who are sources of information relevant to an investigation.

E. Individuals wanted by other law enforcement agencies, including Federal, State, local, tribal, foreign and international, or individuals who are the subject of inquiries, lookouts, or notices by another agency or a foreign government.

F. Individuals, including U.S. Citizens, Lawful Permanent Residents, immigrants and non-immigrants who apply for immigration benefits and/or any form of automated or other expedited inspection for verifying eligibility to cross the borders into the United States.

G. Non-United States citizens and Non-Lawful Permanent Residents who present themselves for entry into and/or exit from the United States, including individuals subject to the requirements and processes of US–VISIT. Individuals covered under US–VISIT include those who are not United States citizens at the time of entry or exit or who are United States citizens or Lawful Permanent Residents who have not identified themselves as such at the time of entry or exit.

H. Individuals unlawfully present in the United States to include persons who have failed to maintain a valid immigration status as well as persons who are otherwise unlawfully present in the United States.

I. Nationals of countries that threaten to wage war, or are at war with the United States, and individuals required to register as agents of foreign governments in the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records come directly from information collected from individuals during DHS or federal enforcement encounters, from information provided by individuals when applying for U.S. immigration benefits or temporary admission to the U.S., or from persons entering or leaving the U.S. Analyzed records include biographical data; biometric identifiers, including fingerprints and photographs; and information or data related to the individual subject's case, including immigration history, alien registration, and other identification or record numbers. The system maintains records used to show relationships across all categories of records. These records include:

A. Information collected from individuals during a DHS enforcement encounter or investigation, including, but not limited to: Names, aliases, dates of birth, phone numbers, addresses, nationality, identification numbers such as A-File Number, Social Security Number, or driver's license number, and physical characteristics. This information is maintained in the Treasury Enforcement Communications System (TECS), last published October 18, 2001, 66 FR 52984 and in the DHS Enforcement Operational Immigration Records (ENFORCE) system, last published DHS/ICE–CBP–CIS–001–03, ENFORCE/IDENT March 20, 2006, 71 FR 13987;

B. Information collected about individuals during a DHS enforcement encounter or investigation, or provided by other State, local, tribal Federal, or foreign law enforcement or other relevant agencies, including, but not limited to: Names, aliases, nationality, dates of birth, phone numbers, addresses, affiliations, identification numbers such as A–File Number, Social Security Number, or driver's license number, or physical characteristics. This information is maintained in TECS;

C. Biographic information such as names, aliases, dates of birth, phone numbers, addresses, nationality, identification numbers such as A–File Number, Social Security Number, or driver's license number, and immigration violation information obtained from the DHS ENFORCE or successor systems;

D. Biographic information such as names, aliases, dates of birth, phone numbers, addresses, nationality, identification numbers such as A–File Number, Social Security Number, or driver's license number, and descriptive information obtained from U.S. Citizenship and Immigration Services (USCIS) immigration benefits applications and application review findings;

E. Information obtained from other Federal or foreign law enforcement agencies about individuals known or reasonably suspected to be or to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

F. Biographic information and other information such as name, address, and phone number obtained from commercial data providers for individuals identified as prospective leads or suspects in active investigations; and

G. Biographic information such as names, aliases, dates of birth, phone numbers, addresses, nationality, identification numbers such as A–File Number, Social Security Number, or driver's license number, and descriptive information obtained from U.S. Customs and Border Protection (CBP) encounters at Ports of Entry during border crossings.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 8 U.S.C. 1103; 8 U.S.C. 1225(d)(3); 8 U.S.C. 1324(b)(3); 8 U.S.C. 1357(a); 8 U.S.C. 1360(b); 19 U.S.C. 1; and 19 U.S.C. 1509.

PURPOSE:

The purpose of the ICEPIC system is to provide the information technology infrastructure products and services that enable investigators and analysts within ICE and other DHS components to recognize non-obvious person, address, and organizational relationships within existing DHS records systems, and to develop timely, actionable leads needed to accomplish ICE law enforcement and counter-terrorism mission objectives. All ICEPIC activity is predicated on ongoing and valid law enforcement investigations. Current manual and automated processes for research, collation, organization, validation, and analysis of the information in numerous DHS alien registration, entry, intelligence, lookout, and enforcement systems can accomplish similar objectives, but are cumbersome, time-consuming, and error-prone. ICEPIC will provide a reliable, responsive, and secure system to support production of actionable leads and law enforcement intelligence for DHS components and other Federal entities, as appropriate and in conformance with this system of records notice.

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 the Privacy Act, 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ) or other Federal agency in the review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which ICE exercises jurisdiction, or when conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS; or (b) any employee of DHS in his/her official capacity; or (c) any employee of ICE in his/her individual capacity, where DOJ or DHS has agreed to represent the employee; or (d) 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 appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of domestic and foreign civil or criminal laws.

C. To U.S. agencies of the national intelligence community or through established liaison channels to selected foreign governments where analysis of the records indicates a potential or confirmed threat of terrorist activity justifying further analysis or investigation.

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. Those provided information under this routine use are subject to the same Privacy Act limitations as are applicable to DHS officers and employees.

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

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. Those provided information under this routine use are subject to the same Privacy Act limitations as are applicable to DHS officers and employees.

G. To appropriate Federal, State, tribal, local, or foreign law enforcement, intelligence, and regulatory agencies, foreign governments, and international law enforcement organizations, for example: the Department of Defense; the Department of State; the Department of the Treasury; the Central Intelligence Agency; the Selective Service System; the United Nations; and INTERPOL; as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to elicit information required to accomplish the purposes described in this paragraph.

H. To an appropriate Federal, State, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence, but only when the disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

I. To an appropriate Federal, State, local, tribal, or foreign government agency, international organization, or private organization where the President or the Secretary of the Department of Homeland Security has declared an event to be a National Special Security Event, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit, but only when disclosure is appropriate to the proper performance of the official duties of the person making the request, and;

J. 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) DHS 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, harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information, or harm to the individual; 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.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Records are stored electronically at one or more ICE data centers that are located in secure facilities. The records are stored on magnetic disc, tape, digital media, and optical media, and may also be retained in hard copy format in secured file folders.

RETRIEVABILITY:

Data are retrievable by an individual's name, Social Security Number, A–File Number, or other unique identifier, as well as by non-identifying information such as address or date of entry into the United States.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS information technology security policies and the Federal Information Security Management Act (FISMA). All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password protection features. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature, which provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties. The system also maintains a real-time auditing log of individuals who access and update the system. Audit logs are reviewed and analyzed for unauthorized and inappropriate system usage. DHS will investigate instances of unauthorized or inappropriate access or use of the system and take appropriate disciplinary actions where violations have occurred.

RETENTION AND DISPOSAL:

The National Archives Records Administration has not yet approved a retention schedule for this system of records. Because a history of Federal law enforcement interactions with

persons and organizations is essential to detecting criminal and terrorist patterns of behavior and locating leads in current investigations, ICE has proposed to retain records in ICEPIC for ten (10) years from ICE's last use of the individual's data, and then archive the information for an additional five (5) years. After the five (5) year period, information will be destroyed unless it has become relevant to a legal action, at which point the retention schedule would reset.

SYSTEM MANAGER(S) AND ADDRESS:

Unit Chief, Program Management Oversight, Mission Support, Office of Investigations, U.S. Immigration and Customs Enforcement, 425 I Street, NW., Washington, DC 20536, telephone: (202) 307–6201.

NOTIFICATION PROCEDURES:

Pursuant to 5 U.S.C. 552a(j) and (k), this system of records may not be accessed by members of the public for purposes of determining if the system contains a record pertaining to a particular individual. Nonetheless persons may seek access to records maintained in ICEPIC as outlined in the Record Access Procedures section below. Requests for such access will be reviewed on a case-by-case basis.

RECORD ACCESS PROCEDURES:

ICEPIC is exempt from record access procedures pursuant to 5 U.S.C. 552a(j) and (k). Nonetheless persons may seek access to records maintained in ICEPIC by contacting U.S. Immigration and Customs Enforcement Freedom of Information Act Office, 800 North Capitol Street, NW., Room 585, Washington, DC 20536. Individuals must submit their request and use the form found at *http://www.ice.gov/doclib/g-639.pdf*. Requests for such access will be reviewed on a case-by-case basis to ensure that the records meet the requirements set out by the Privacy Act.

CONTESTING RECORD PROCEDURES:

This system is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4) (G) and (H), and (f) pursuant to 5 U.S.C. 552a(j)(2), (k)(2); however, requests for amendment of records may be reviewed on a case-by-case basis. Follow the ''Record Access Procedures'' noted above.

RECORD SOURCE CATEGORIES:

Information contained in the system is obtained from DHS investigators, other DHS law enforcement officers, other Federal, State, foreign and tribal law enforcement and intelligence agencies, public records, commercial data aggregators, and immigration and alien admission records systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt 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)(1), (e)(4)(G), (e)(4)(H), and (f). In addition, to the extent a record contains information from other exempt systems of records, ICE will rely on the exemptions claimed for those systems.

Dated: August 11, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–19031 Filed 8–15–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2007–0054]

Privacy Act of 1974; United States Citizenship and Immigration Services; Fraud Detection and National Security Data System (FDNS–DS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: The USCIS has developed the Fraud Detection and National Security Data System (FDNS–DS), a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns.

DATES: Written comments must be submitted on or before September 17, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2007–0054 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, 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: United States Citizenship and Immigration Services, Privacy Officer, Donald Hawkins, 111 Massachusetts Avenue, NW., Washington, DC 20529. For privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Office of Fraud Detection and National Security (FDNS) of the United States Citizenship and Immigration Services (USCIS) has developed a new system named the Fraud Detection and National Security Data System (FDNS–DS). FDNS–DS is a central repository that permits specially-trained employees to record, track, and manage the background checks and adjudicative processes related to immigration applications and petitions with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments (BFAs). The system will also have the capability to track the following:

1. USCIS investigative referrals to law enforcement agencies (LEAs);
2. LEA referrals to USCIS concerning subjects with pending immigration benefit applications or petitions;
3. background check referrals and resolutions associated with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns; and
4. any additional inquiries conducted in order to confirm that the information on file is correct.

FDNS has created FDNS–DS, a centralized data system, in order to increase the effectiveness of United States (U.S.) immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. With the implementation of FDNS–DS, USCIS's capabilities for detecting and tracking