Privacy Impact Assessment
for the

ICE Pattern Analysis and Information Collection (ICEPIC)

January 25, 2008

Contact Point
Marcy Forman
Director
Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 514-0078

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(702) 235-0780

Abstract

U.S. Immigration and Customs Enforcement (ICE) has established a system called the ICE Pattern Analysis and Information Collection (ICEPIC) system. ICEPIC is a toolset that assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. All ICEPIC activity is predicated on ongoing law enforcement investigations. This privacy impact assessment is being completed to provide additional notice of the existence of the ICEPIC system and publicly document the privacy protections that are in place for the ICEPIC system.

Introduction

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 are tasked with identifying and understanding the relationships between individuals, places, and items that are the subject of investigation. ICE currently 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.

ICE has established a system known as the ICE Pattern Analysis and Information Collection (ICEPIC) system. 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 will develop specific leads and intelligence for active and new investigations. Identified relationships will also be recorded for reuse in subsequent investigative analyses. The information processed by ICEPIC will come from existing ICE investigative and apprehension records systems, as well as immigration and alien admission records systems. ICEPIC includes capabilities that assist investigators in recording results of analyses performed in support of investigations and in capturing 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 government agencies, or international organizations.

ICEPIC is a set of information analysis tools which allow disparate sources of information to be analyzed to find previously unknown relationship data about individuals who are the subject of ongoing and valid investigations. Relationship data is made up of information about how a place, person, or thing (e.g., automobile or other piece of property) relates to other persons, places, or things. For example, ICEPIC can determine relationship data about how certain events occurred at a certain address, or certain individuals under investigation who have shared the same address in the past. ICEPIC also includes capabilities that assist investigators in recording results of analyses performed in support of investigations. All ICEPIC searches are conducted with the appropriate predicate for a search, i.e., ongoing investigation into a violation of law.

There are two categories of information flowing in or through ICEPIC at any time: source information brought in from existing systems of records (see Question 1.2), and ICEPIC analytical reports produced by ICEPIC users.

Sources of Information

ICEPIC is structured to allow information from several different sources to be analyzed simultaneously. The information within ICEPIC comes from existing systems of records owned by DHS and non-DHS agencies (see Question 1.2). The information arrives in ICEPIC either by direct electronic connection or regular manual electronic upload (e.g., CD-ROM). The information in ICEPIC is taken from the backup data (where applicable) of the source systems. The data is stored directly in ICEPIC.

Analytical Reports

Initially, an agent/analyst queries the available data using ICEPIC. The results are presented in a manner that identifies relationships among different individuals or among records from different sources for the same individual based on the specific agent/analyst's search criteria. An agent may then consult a commercial database in order to complete missing data in the available information. Because ICEPIC presents available information to an agent/analyst, but does not analyze for relevance outside of the search criteria, all of the information is then analyzed by ICE agents/analysts. This analysis involves determining which information is relevant to the investigation and which is not, meaning that analysts disregard irrelevant data returned from a search. The relationship searches are saved in a separate database within ICEPIC along with a formal and final analytical report which is prepared and filed by the agent/analyst.

For example, a request or lead may come to ICE for additional biographic and address information on a particular individual identified as a subject, lead, or associate in an investigative case. The assigned ICE agent/analyst uses ICEPIC to locate any relevant information that exists and identify anyone else who may share the same information in ICEPIC. The agent/analyst further verifies the information through government source databases or through commercial data sources and through contacts with other government agents to ensure accuracy or to complete the missing information. An analytical report indicating the research findings of the ICE agent/analyst is compiled and provided to the requesting agency.

Information collected by ICEPIC is integral to active ICE law enforcement investigations and is directed at developing new leads for those investigative cases. It is also used to identify relationship patterns that are indicative of violations of U.S. customs and immigration laws and possible terrorist activities, potentially resulting in the opening of new investigative cases.

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

The information in ICEPIC consists of the biographical and biometric information obtained from individuals during DHS enforcement encounters or provided by individuals when applying for U.S. immigration benefits or admission to the U.S. Biographical data includes name, aliases, date of birth, phone numbers, addresses, and nationality; biometric information includes fingerprints and photographs. Prior law enforcement encounter information consists of data related to an individual's case, including immigration history, alien registration information, and other identification or record numbers.

Agents/analysts may consult commercial data providers in order to verify information within ICEPIC. As a specific example, an agent/analyst investigating a lead may encounter a gap in residential addresses for a

particular individual. The agent/analyst may consult a commercial data provider to search for the missing address. How much weight to give the information from commercial data provider is left to the professional discretion of the agent/analyst.

Additionally, ICEPIC separately retains the relationship information identified using ICEPIC and the analytical reports created by the investigating analyst or agent.

1.2 From whom is information collected?

The information processed by ICEPIC is supplied by other DHS law enforcement systems of records. ICEPIC does not directly collect information from individuals.

Generally, Enforcement Operational Immigration Records (ENFORCE)(last published DHS/ICE-CBP-CIS-001-03, Enforce/IDENT March 20, 2006, 71 FR 13987) and Treasury Enforcement Communications System (TECS) (last published October 18, 2001, 66 FR 52984) information is collected directly from individuals during an encounter with DHS. Other data are obtained directly from persons applying for U.S. immigration benefits or admission to the U.S. This information is collected by the DHS Student and Exchange Visitor Information System (SEVIS)(last published March 22, 2005, DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS), 70 FR 14477), National Security Entry Exit Registration System (NSEERS), the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system Arrival and Departure Information System (ADIS) (last published August 22, 2007, DHS/USVISIT-001, 72 FR 47057), and the U.S. Citizenship and Immigration Services (USCIS) immigration benefits applications and application review systems, including the A-file (last published January 16, 2007 DHS/USCIS-001 Alien File and central Index System, 72 FR 1755) and Claims 3 and Claims 4 information (last published October 17, 2002 Justice/INS-013 INS Computer Linked Application Information Management System (CLAIMS), 62 FR 59734).

A much smaller set of information is obtained from other Federal law enforcement agencies about individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

Additionally, information from commercial databases may be used to verify information or resolve gaps in investigative reports.

1.3 Why is the information being collected?

ICEPIC does not directly collect information from individuals. ICEPIC uses the information collected by other entities to aid law enforcement investigations related to violations of U.S. customs and immigration laws and to accomplish the DHS counterterrorism mission.

1.4 How is the information collected?

ICEPIC is not the initial collector of any information it receives. However, information collected in other databases is received by ICEPIC through direct electronic transmission and manual upload from CD- or DVD-ROMs. Information is collected either via physical disc or direct electronic connection.

Commercial data provider access is not direct. Information is referenced and copied over to ICEPIC if necessary. No formal data exchange occurs. Commercial data is not directly downloaded into ICEPIC; rather an agent/analyst must, if necessary, copy the information specific to a particular query or search.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

ICE has been authorized to collect information under 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.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

ICEPIC does not directly collect information. ICEPIC only analyzes information collected by other systems. ICEPIC's toolset for examining relational data is intended to be used for a very specific purpose by DHS. ICE will be analyzing only the information needed to support investigations of violations of U.S. customs and immigration laws and potential terrorist activities and threats. Controls implemented for ICEPIC users ensure that the use of ICEPIC remains limited to ICE and DHS missions.

A privacy risk is presented by having an information technology system make decisions about the relevance or value of data being searched. This is mitigated by the fact that agents/analysts are a) conducting searches based on appropriate legal predicate, b) submitting search parameters within that appropriate predicate, and c) reviewing any and all results displayed by ICEPIC. Human review of the relevance and quality of data provides a measure of protection against unreasonable links made by a computer's analysis. This ensures that human agent/analysts are responsible for any ultimate investigative decisions, not ICEPIC. The human review is also effective in the use of commercial data, which allows for an agent/analyst to verify information from ICEPIC.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

All source information is used to generate analytical reports to identify potential violations of customs or immigration law, confirm suspected violations, or investigate potential terrorist threats. ICEPIC will assist ICE investigators by automating five business processes:

1. Analysis of leads, law enforcement and intelligence reports, and referrals, and processing of queries of ICE and DHS information to locate relevant records and produce reports.
2. Integration and resolution of information from multiple ICE and DHS databases to provide leads for law enforcement investigations and disruption of potential terrorist activities.
3. Initiation of analyses that support investigative cases in ICE headquarters and field offices and recording of the results of beneficial analyses.
4. Production and dissemination of target indicator profiles and other intelligence.
5. Management of analysis workflows and information resources.

Reports generated through the use of information in ICEPIC are used by the Department of Justice (DOJ) or other federal agencies 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 that is acting in his or her official capacity in support of ICE, the United States, or any agency thereof is involved. The Federal Bureau of Investigation (FBI) uses ICEPIC information when ICE becomes aware of information that may be related to an individual in terrorism-related activity.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

ICEPIC provides the information technology that will enable ICE investigators and analysts to recognize non-obvious relationships among persons, resolve addresses collected in varied formats, understand organizational relationships using information within existing DHS record systems, and develop timely, actionable leads needed to accomplish ICE law enforcement objectives.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information is not directly collected from individuals. ICEPIC only uses information collected by other systems. Because of the law enforcement context in which ICEPIC is used, it may often be impossible to directly verify the accuracy of information with the individual about whom the specific information pertains. However, because ICEPIC supports all DHS enforcement activities, users other than the data owner who hold relevant knowledge have the opportunity to correct inaccuracies when they come to their attention. Furthermore, user training and standard operating procedures emphasize the importance of verifying information prior to including it in analytical reports. Verification procedures include direct queries to source DHS enforcement and immigration databases, other government databases, and ICE agent interviews with subjects of interest. If necessary an agent/analyst may consult a commercial data provider to verify information.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

As described in Section 8 of this document, security and access controls and audit processes are in place to mitigate the risk that personal information will be accessed by unauthorized individuals. ICEPIC users receive computer security and privacy awareness training to mitigate the risk that information will be used inappropriately.

A risk exists that ICEPIC, and not human agents/analysts, is making important decisions about investigations and individuals; that ICE is ceding control of investigations to a non-human entity. This is not true of ICE or ICEPIC. ICEPIC makes no decisions regarding significance of relationships; it simply identifies possible connections for law enforcement officers to investigate. Likewise, ICEPIC does not determine accuracy of data from its source systems; rather, the validity of data or relationships identified by ICEPIC must be verified by the agents/analysts. The risk that incorrect information will be used to make decisions regarding individuals is mitigated by policies requiring law enforcement officers to be trained to verify information before including the information in an analytical report, and standard procedures requiring officers to record the information verification process and findings in their reports. Those reports are stored separately in ICEPIC.

Section 3.0
Retention

3.1 What is the retention period for the data in the system?

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.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

ICE has not yet established a NARA-approved retention schedule for ICEPIC records.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The ten (10) year period suggested for ICEPIC complements the mission requirements of ICEPIC because ten years allows for sufficient time to analyze any broader criminal trends or behaviors, and would also allow for a fuller development of complicated cases where linkages between subjects, organizations, and criminal conspiracies is difficult to detect. Likewise criminal organizations themselves take a number of years to fully develop and continue to evolve over time. Information ICE gathers regarding one individual involved in the earlier stages of such an organization would continue to have significance over the course of the organization's development and evolution. Understanding that the retention period should not be longer than the mission and purpose of the system, ten (10) years ensures that ICE can use the information for the stated purpose while not keeping the information longer than necessary.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

Based on need to know, ICE may share analytical reports generated from ICEPIC information with other parts of DHS including both law enforcement and intelligence agencies. These may include: the DHS Operations Center, U.S. Secret Service, the U.S. Coast Guard, U.S. Customs and Border Protection, Transportation Security Administration, and the Office of Intelligence and Analysis. Organizations will only receive the information which they are authorized to receive.

It is important to note that information is shared only one-way; ICEPIC receives information but does not send information back to other DHS law enforcement systems. ICEPIC only shares analytical reports with DHS law enforcement and intelligence agencies that have a need to know. ICEPIC does not share raw data.

4.2 For each organization, what information is shared and for what purpose?

ICE shares analytical reports (not raw data) generated from ICEPIC information with intelligence and law enforcement officials within DHS for the purpose of investigating violations of the customs and

immigration laws, as well as possible terrorist threats and plots. Any analytical report from ICEPIC has the potential to be shared with other authorized DHS components. The information will be shared to the extent that the DHS component has demonstrated a need to know and the use for the information falls within that component's statutory mission.

4.3 How is the information transmitted or disclosed?

Information is transmitted via DHS e-mail or it is hand-delivered to DHS special agents, supporting analysts, supervisors, and other authorized DHS law enforcement, immigration benefits, intelligence, and counterterrorism agencies. All recipients of the information are required to be trained in the Privacy Act (and Executive Order 12333 for the intelligence community, where applicable) and in appropriate uses and disclosure controls pertinent to the information. All information is encrypted during transmission.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

A risk exists that information may be shared with DHS components without a need to know. Information from ICEPIC is shared only with DHS law enforcement organizations that have a role in the investigation of possible violations of the customs and immigrations laws enforced by DHS agencies and possible terrorist threats and plots. As described in Section 8 of this document, ICEPIC uses access controls and audit trails to mitigate the risk that information will be accessed by unauthorized individuals or improperly used by authorized individuals. Users receive security and privacy training, and this helps mitigate the risk that information will be used inappropriately. This also mitigates the risk that the information will be provided to individuals without a need-to-know.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

ICE shares analytical reports (not raw data) generated from ICEPIC information with law enforcement or intelligence agencies that demonstrate a need to know the information in the performance of their missions, including Federal, State, tribal, local and foreign law enforcement agencies, as well as relevant international organizations such as INTERPOL. As mentioned above, DOJ and the FBI will receive analytical reports regularly, but external sharing is not limited to those agencies. All sharing is in accord with the ICEPIC System of Records Notice and the Privacy Act.

It is important to note that information is shared only one-way; ICEPIC receives information but does not send information back to these systems. ICEPIC only shares analytical reports with agencies that have a need to know. ICEPIC does not share raw data.

Prior to taking on new source data, a Memorandum or Letter of Understanding (MOU or LOU) is generated with the partner agency to ensure all requirements are met for security and privacy. If the new data set is owned by ICE or another DHS component an interagency service agreement (ISA) is executed which also covers security and privacy.

5.2 What information is shared and for what purpose?

As required by the Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002), Homeland Security Information Sharing MOU of March 4, 2003, and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 25, 2005, analytical reports are shared with the FBI when ICE becomes aware of information that may be related to an individual identified as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. This sharing is in accord with the routine uses published in the ICEPIC System of Records Notice.

Reports are also shared with any Federal law enforcement or intelligence agency that demonstrates a need to know to further its own law enforcement analyses or investigations.

5.3 How is the information transmitted or disclosed?

Information is transmitted via hand-delivered reports and via e-mail over DHS sensitive but unclassified (SBU) networks, the DHS Homeland Security Data Network (HSDN), and the Department of Defense's Secret Internet Protocol Router Network (SIPRNET).

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

ICE does not anticipate giving outside agencies direct access to ICEPIC. Accordingly, no MOU or Memorandum of Agreement (MOA) is deemed necessary. ICEPIC analytical reports will be distributed on a case-by-case basis to authorized Federal law enforcement and intelligence agencies consistent with the reason for collection of the source information and the routine uses that are to be published in the ICEPIC System of Records Notice (SORN).

Pursuant to the Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002), Homeland Security Information Sharing MOU of March 4, 2003, and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 25, 2005, analytical reports are shared with the FBI when ICE becomes aware of information that may be related to an individual identified as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

Other routine law enforcement uses of ICEPIC information are as follows: to a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, 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 information and intelligence.

5.5 How is the shared information secured by the recipient?

Reports are marked as "For Official Use Only/Law Enforcement Sensitive." As a pre-condition to receiving such reports, ICE prohibits the recipient agency from further disseminating the information without prior approval from ICE.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

Information users in government organizations outside DHS typically complete information security training.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

A risk is presented that information may be delivered to agencies outside of DHS that do not have a need to know ICEPIC information. Information in ICEPIC is shared only with law enforcement and intelligence organizations that have demonstrated a need to know the information in the course of their official duties. Security and Privacy Act training also mitigate the risk that sensitive information will be handled improperly. Additionally, it is ICE policy that information deemed "Law Enforcement Sensitive" may not be further distributed without the prior consent of the originator.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

ICEPIC does not directly collect information from individuals. ICEPIC analyzes information collected by other systems. This Privacy Impact Assessment (PIA) and the ICEPIC SORN (published concurrently with this PIA) serve as public notice of the ICEPIC system. With respect to the originating information obtained from immigration benefits applications, such individuals are notified through notices contained on the benefits applications that their information may be shared with law enforcement entities. As part of this PIA and SORN process, DHS reviewed the applicable SORNs to ensure that the uses were appropriate given the notice provided.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

ICEPIC collects no information directly from individuals. The information is collected by other systems. In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, opportunities to decline may be limited or nonexistent.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, no such consent exists.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

A risk exists that the public is not aware of ICEPIC, or, that individuals may not be aware that their information may be contained within ICEPIC. Most directly the public is provided notice of the ICEPIC system through this PIA and the SORN. As part of this PIA and SORN process, DHS reviewed the applicable SORNs to ensure that the uses were appropriate given the notice provided.

Further, because ICEPIC is a system where many law enforcement or intelligence contexts apply, notice or the opportunity to consent to use would compromise the ability of the agencies to perform their missions and could put law enforcement officers at risk. Thus, notice of collection and consent to specific uses are not available in most cases for ICEPIC.
Because access to the records contained in this system of records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency, access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by on investigative agencies. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

Section 7.0
Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

As noted in the SORN and the Notice of Proposed Rulemaking (NPRM) for the Privacy Act exemptions, DHS is exempting the records from general access provisions pursuant to 5 U.S.C. 552a (j) and (k). Nonetheless, persons may seek access to records maintained in ICEPIC. Individuals can submit a Freedom of Information Act (FOIA) request or Privacy Act request using the form and procedures outlined on the ICE web page 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.

7.2 What are the procedures for correcting erroneous information?

A person who, having accessed his or her records in ICEPIC, wishes to contest or seek amendment of those records should direct a written request to the Office of Investigations, Information Disclosure Unit, 425 I St., NW, Washington, DC 20536. The request should include the requestor's full name, current address, and date and place of birth, as well as a copy of the record in question and a detailed explanation of the change sought. As noted above, DHS has exempted the system from access and redress; however, requests for amendment of records may be reviewed on a case-by-case basis.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure appears in the ICEPIC SORN published concurrently with this PIA.

7.4 If no redress is provided, are alternatives available?

If an individual is not satisfied with the response, he or she can appeal his or her case to the appropriate authority provided for in the FOIA process.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction, and redress rights are not provided please explain why not.

A risk is presented that individuals are not aware of their ability to make record access requests for records in ICEPIC. Individuals can request access to information about them through the FOIA process and may also request that their information be amended by contacting the ICE, Office of Investigations, Information Disclosure Unit, 425 I St., NW, Washington, DC 20536. The nature of ICEPIC and the data that it collects, processes, and stores is such that the ability of individuals to access or correct their information will be limited. However, outcomes are not predetermined and each request for access or correction is individually evaluated.

Because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency, access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden on investigative agencies. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security. Nonetheless, persons may seek access to records maintained in ICEPIC as outlined in the Record Access Procedures of the SORN. Requests for such access will be reviewed on a case-by-case basis.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

The primary user groups having access to the system are ICE law enforcement agents and analysts. Other groups have limited access, including contractors working with ICE who are responsible for developing the system and ICE government and contractor information technology operations and support staff.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors will have access to all systems, including ICEPIC developers and information technology operations and maintenance staff.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Each user account is assigned certain roles. Each of these roles has a set of privileges defined for it. The ICEPIC administrator can elect to assign all the privileges for a given role or can select only certain privileges to assign.

8.4 What procedures are in place to determine which users may access the system and are they documented?

ICE Office of Investigations management is responsible for ensuring that all personnel are appropriately monitored in ICEPIC. This is done by working with the ICEPIC administrator to establish user accounts as users are assigned to access ICEPIC and to update user identification, role, and access profiles as changes are needed. Users will be provided appropriate training and guidance regarding this process.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Access roles are assigned by a supervisor and implemented by an administrator. Access roles are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access are removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Audit trails are used to track user activities and provide accountability. These activities include data access, modifications, and deletions. Only authorized personnel have access to audit logs and they are kept for a minimum of 90 days. Audit trails and/or audit logs are reviewed by ICEPIC System Administrators or the Information Systems Security Officer (ISSO). The system administrator maintains a spreadsheet record of the receipt or distribution of sensitive information on electronic media and is responsible for restricting access to output products. Also, any violation or criminal activity is reported to the Office of the Information System Security Manager (OISSM) team in accordance with the DHS security standards, as well as the ICE Office of Professional Responsibility. The same module that manages roles and permissions is designed to automatically detect unauthorized activities.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

The ICE OISSM provides initial and annual Computer Security Awareness Training with an online training and testing application. This training addresses protecting sensitive information. Every employee that accesses the system must sign a "Rules of Behavior" agreement, which includes protecting sensitive

information from disclosure to unauthorized individuals or groups, after passing the background investigation.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The ICEPIC security Certification and Accreditation (C&A) was awarded in November 2005. The system will be secured in accordance with DHS and national-level security requirements, including FISMA requirements.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The risk that personally identifiable information will be used inappropriately is mitigated by security training that discusses how to protect sensitive information and by the use of audit mechanisms that log and monitor user activity. The assignment of roles to users to establish their access requirements, based on their functions and regular review of those roles, mitigates the risk that users will be able to access information they are not required to access. All systems have been through a system security certification and accreditation process that reviews those security mechanisms and procedures that are in place, and ensures they are in accordance with established policy.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

ICEPIC consists of Government Off-the-Shelf (GOTS), Commercial Off-the-Shelf (COTS), and custom-developed applications and databases.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy, and security are important parts of the decisions made for the ICEPIC system, and evidence of this can be seen in the procedures used to protect the system. The ICEPIC system secures information by complying with the requirements of the DHS Information Technology Security Program Handbook. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and applications rules that are applied to systems and communications between systems.

9.3 What design choices were made to enhance privacy?

The use of access controls and audit trails are design choices employed in order to enhance privacy.

Conclusion

Using ICEPIC, ICE law enforcement agents and analysts will 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 will develop specific leads for active and new investigations. Identified relationships will also be recorded for reuse in subsequent investigative analyses. The information processed by ICEPIC will come from existing ICE investigative and apprehension records systems, as well as immigration and alien admission records systems.

Because some of the information processed by ICEPIC is collected by law enforcement agencies in field situations and because of the investigative context in which ICEPIC is used, it may be difficult or impossible to directly verify the accuracy of information with the individual or organization to whom it pertains. However, because ICEPIC supports all DHS law enforcement activities, users who hold relevant knowledge have the opportunity to correct inaccuracies when they come to their attention. Furthermore, user training and standard operating procedures emphasize the importance of verifying personal and organization information prior to acting upon it.

The privacy risk for new data is also mitigated by the fact that ICEPIC has in place effective security mechanisms, including access controls and auditing mechanisms. In addition, ICE has procedures in place in the areas of notice, redress, access, and correction. Information is shared only with internal and external government organizations that play a role in law enforcement and homeland security and demonstrate a need to know. All of these mechanisms combine to create a process with effective privacy protection.

Responsible Officials

Marcy Forman, Director
Office of Investigations
U.S. Immigration and Customs Enforcement

Approval Signature Page

Original signed and on file wit the DHS Privacy Office.

Hugo Teufel III

Chief Privacy Officer

Department of Homeland Security