Privacy Impact Assessment
for the

ICEGangs Database

January 15, 2010

Contact Point
Kumar Kibble
Acting Director, Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) owns ICEGangs, a gang-tracking software application used for investigative, analytical, and statistical recording and tracking of gang members and associates, gangs, and their activities. The ICEGangs database supports information sharing on gang members and activities among participating law enforcement agencies. ICE is conducting this Privacy Impact Assessment because the system collects and maintains personally identifiable information (PII).

Overview

ICEGangs is based on the commercially developed GangNET software tailored to include immigration status-related information and is similar to other versions of GangNET utilized by numerous federal, state and local law enforcement agencies across the United States and Canada. ICEGangs is managed by the ICE Office of Investigations (OI) under the National Gangs Unit.

ICEGangs has two main purposes. First, it supplements the existing ICE case management system by providing a consolidated repository of information on gang members and associates and gang-related activity. ICEGangs allows ICE agents and support personnel to search gang-oriented information in a more efficient and effective manner than is possible in ICE's standard investigative case management system. For example, an ICE field agent can easily query ICEGangs for a list of members in a specific gang. It is not currently possible to perform the same sort of query using ICE's case management system. As a matter of policy, ICE agents are required to create and/or update ICEGangs records for suspected and/or confirmed gang members and associates whenever they encounter gang members and associates in the field during their official law enforcement activities. ICEGangs records also contain references to the official evidentiary system of records, which allows ICE agents and support personnel to refer to official case records.

Second, ICEGangs facilitates the sharing of gang information between ICE and other law enforcement agencies. In particular, ICE currently provides the California Department of Justice (CalDOJ) access to the data in ICEGangs. CalDOJ users access the ICEGangs repository remotely through their own CalGangs application. In the future, ICE anticipates that it will share information with other state and local law enforcement agencies that use the GangNET software. ICE will require access controls for state and local agencies as a prerequisite to gaining access to ICEGangs data.

ICEGangs complies with 28 Code of Federal Regulations (C.F.R.) Part 23, a federal regulation governing Federally funded multijurisdictional criminal intelligence systems to ensure they are used in conformance with the privacy and constitutional rights of individuals. Under this regulation, a project can only collect and maintain criminal intelligence information concerning an individual if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. Also, a program must establish system submission criteria that define which individuals will be recorded in the system. All systems operating under 28 C.F.R. Part 23 have a mandatory maximum retention period of five years after the last date the data is accessed.

In accordance with 28 C.F.R. Part 23, an individual must meet criteria established by ICE to be included as either a gang member or gang associate in ICEGangs. For example, an individual that has been convicted of a gang-related offense, has admitted to gang membership, and/or has been identified as a gang member by a jail or prison in which they were confined, would be included as a gang member or associated in the ICEGangs system.

ICEGangs data is not used directly as evidence to prosecute crimes. ICEGangs is solely a data repository with limited search and analytical tools that help ICE agents identify individuals and organizations that may be involved in gang-related criminal activity. It is incumbent on the investigator that uses ICEGangs to build their case using original data sources which are referenced in ICEGangs.

Typical Transaction

During the course of a criminal investigation, an ICE agent encounters an individual (for example, the agent interviews the individual) who meets the ICE-established criteria for being a gang member. In addition to other recordkeeping activities associated with the investigation (e.g., writing a report of interview for the case file and inputting information into the ICE case management system), the agent will also logon to ICEGangs and query the system to determine if the individual already has an ICEGangs record. If no record exists, the agent will create a new record and enter the available identifying information about the individual, such as name, date of birth, physical description, immigration status, suspected gang affiliation, and photograph if available. The agent will also enter notes about his encounter with the individual (i.e., the interview). If the individual already has an ICEGangs record, the agent will review the record to determine if there is any useful information that may assist in his current investigation. In addition to updating any official case records that exist pertaining to the current investigation, he will also update the ICEGangs record with any new information obtained during the interview and will enter notes about the interview itself.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

ICEGangs maintains personal information about individuals who qualify as suspected or confirmed gang members and associates under ICE criteria. ICEGangs stores the following data about each gang member and associate to the extent it is available: biographic information (name, date of birth, etc.), immigration status, gang affiliation, physical description, government-issued identification numbers, photos of the individual, identities of gang associates, field interview notes, and criminal history information. ICEGangs also stores general comments entered by the ICE agent that created the gang

member or associate record as well as a reference to the official evidentiary system of records where official case files are stored.

ICEGangs maintains more general data on criminal gangs including gang names, various symbols they use, membership levels, and turf claimed. Each subject record in ICEGangs also includes the contact information for the ICE agent that entered the information into ICEGangs so that they can be contacted, if necessary, by other ICEGangs users.

Finally, ICEGangs users can quickly generate various reports such as gang rosters or statistical reports on demographics, and link analysis reports that identify commonalities between records in ICEGangs based on user-defined queries and criteria. Statistical reports do not contain any personal information about gang members. These reports are user-generated on an ad hoc basis and are not stored in the system for future use. These reports can be printed.

1.2 What are the sources of the information in the system?

ICE agents obtain information such as statements or seized communications[1] about gang members and/or associates directly from the individual or from other suspects, witnesses, informants, and victims during normal law enforcement investigative activities such as arrest, search, or field interview. ICE agents and support personnel may also collect and input into ICEGangs information from other law enforcement agencies so long as that agency's information satisfies ICE criteria for designating an individual as a gang member or associate.

ICEGangs users also have access to the records of other organizations that use the GangNET software. Currently, ICE is only able to access data from CalDOJ's CalGangs application. In the future, ICE anticipates accessing gang data from a variety of state and local law enforcement agencies, via its existing connection to CalGangs.

1.3 Why is the information being collected, used, disseminated, or maintained?

The ICEGangs database supplements the existing ICE case management system in that it allows ICE agents and support personnel to efficiently search, access, and review gang-related information in support of law enforcement investigations. Currently, the ICE case management system is not designed to consolidate and organize investigative materials about gang-related activity or to facilitate sharing of gang-related information with other law enforcement agencies. ICEGangs provides a central repository for all ICE field offices to use to enter, search, and analyze information about gangs, gang activities, and gang members and their associates.

The information is also maintained to allow the sharing of gang information with other law enforcement agencies in support of criminal investigations and related activities. At present, ICEGangs

[1] A seized communication might be the contents of a cell phone or pager, documents identified at a crime scene or in the possession of a suspect, etc.

only shares information with CalDOJ. ICE may share in the future with other state and local law enforcement entities.

1.4 How is the information collected?

ICE agents collect the information directly from individuals during normal law enforcement investigative activities such as an arrest or field interview, from an informant, or by reviewing documentary evidence such as seized communications. ICE agents and support personnel also collect information from prisons about gang members in their populations on an ad hoc basis. Periodically, ICE receives data on gang members and associates from other law enforcement organizations, which it then enters into ICEGangs. Data collection from other law enforcement organizations is not routine and currently takes place on an ad hoc basis.

Before an ICEGangs user creates a new record, the ICEGangs software automatically queries the existing records and allows the user to update an existing subject record rather than creating a new record. This reduces the likelihood of duplicate subject records.

Likewise, information in CalGangs is collected under similar circumstances by law enforcement personnel employed by the CalDOJ. CalGangs uses the same software as ICEGangs so the method of entry (including the provisions for preventing subject record duplication) is identical.

1.5 How will the information be checked for accuracy?

ICE agents and support personnel entering information into the ICEGangs database are trained on the identification and verification of suspected gang members and associates and only enter a subject into the database once the individual has been determined to satisfy the ICE gang member/associate criteria. It is under the discretion of trained ICE agents and support personnel to determine whether an individual meets these criteria and is entered into the ICEGangs database. At least once per calendar year, the system administrator will query a sample of ICEGangs records and check them for accuracy by contacting the originating office and verifying the information.

Additionally, ICEGangs automatically queries existing records before allowing the user to create a new subject record so there is usually only one record per individual in ICEGangs. The subject's record is updated, expanded, and corrected each time the subject is encountered by an ICE agent, which improves the accuracy of the information.

As a safeguard, if ICEGangs data is found to be helpful in the context of a current investigation, ICE agents are required to obtain and verify the original source data from the agency, whether it is another ICE agent or another agency, that collected the information, rather than relying solely on the information in ICEGangs, to prevent inaccurate information from being relied upon during the investigation and any subsequent trial.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

ICE has been authorized to collect this 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.

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

Privacy Risk: ICEGangs may contain records about individuals who are neither gang members nor associates.

Mitigation: This risk is mitigated by having automatic purge parameters in place which permanently deletes stored PII if that information has not been accessed within five years, in accordance with 28 C.F.R. Part 23. Furthermore, every user of ICEGangs undergoes agency-wide and system-specific training as described in Question 8.3 to ensure they conform with all policies pertaining to the system.

It is important to note that ICEGangs data is never used directly as evidence to prosecute crimes. ICEGangs contains references to the official evidentiary systems of records, which makes it possible for agents to verify the accuracy of information before taking action based on that information. ICEGangs is solely a data repository with limited search and analytical tools that help users identify individuals and organizations that may be involved in gang-related criminal activity. It is incumbent on the investigator who uses ICEGangs to fully check all original data sources. As a safeguard, when investigating potential violations of U.S. laws ICE investigators are required to obtain and verify the original source data from the agency that collected the information to prevent inaccurate information from propagating.

Privacy Risk: There is also a risk that ICEGangs collects more information than necessary for the purpose of the system.

Mitigation: For ICEGangs to be effective, it must contain as many details on gangs and gang members and associates as possible so that users can search the database for the individuals or organizations they are researching. Systems used for law enforcement purposes typically require more information than non-law enforcement systems to serve their purpose. This risk is mitigated by the limited retention period (five years from the date of last record activity) for information about individuals.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

ICE uses the gang member and associates information stored in ICEGangs to support the centralized storage, retrieval, research and analysis of this information among various ICE field offices. ICE agents use ICEGangs for various purposes in connection with criminal law enforcement investigations and other law enforcement activities. For example, an ICE agent may search ICEGangs to determine whether an individual who is the subject of an ongoing criminal investigation is associated with gang activity. Such information may reveal to the agent a connection between the crimes being investigated and gang activity, which could help refocus the investigation. The agent may also use ICEGangs to identify the individual's known gang associates or fellow gang members who may be witnesses, suspects, or accomplices to the crimes being investigated. ICEGangs users are also able to see the other personnel who encountered the ICEGangs subject, which may facilitate information sharing pertaining to the investigation or prosecution of a particular individual or case.

ICE also uses ICEGangs to electronically share gang information between ICE and CalDOJ through reciprocally connected GangNET software. Through their own CalGangs application, CalDOJ users can query and obtain read-only access to the ICE data in ICEGangs. ICE users can also access CalGangs information in the same way by querying the ICEGangs system.

ICE also uses ICEGangs to produce statistical reports on gang activities for various law enforcement, management, and reporting purposes. ICEGangs also allows users to conduct link analysis among the various records to identify individuals that may be connected by an attribute such as an address or an associate. These connections and associations may provide leads for ICE agents to follow in pending investigations. ICEGangs users can also quickly generate gang rosters identifying all members of a particular gang.

ICEGangs data is never used directly as evidence to prosecute crimes. ICEGangs is solely a data repository with limited search and analytical tools that help ICEGangs users identify individuals and organizations that may be involved in gang-related criminal activity. It is incumbent on the investigator that uses ICEGangs to fully check all original data sources. The only exception to this is that ICEGangs has the capacity to create photographic lineups. These photographic lineups may be shown to witnesses or victims to aid in the identification of suspects.

2.2 What types of tools are used to analyze data and what type of data may be produced?

ICEGangs has a query interface called "Find Subject" which provides users the capability to search over 50 unique field types against ICEGangs subject records. For example, a list can be generated searching all subjects with a tattoo on the front side of their left leg. From that list another ICEGangs

tool, the photo line-up, can be used to produce a series of photos of gang members or associates from the list of search results. The user can save the lineup in ICEGangs or print it to help witnesses and victims identify suspected gang members or associates.

Additionally, ICEGangs includes many standardized statistical reports that provide aggregate counts based on the report type. These reports are pre-programmed and require a user to supply basic criteria such as age, gender, or ethnic background. The ad-hoc query reports allow users to create and save custom query templates that are not already included in ICEGangs. Users can construct their own reports using any information contained in the database. These reports are built using standard structured query language (SQL).

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

ICE agents that collect information about a gang member or associate in the course of an investigation or other law enforcement activity may obtain some of that information from commercial or publicly available data sources. That information may ultimately be entered into ICEGangs when the gang member or associate record is created or updated by the agent. The agent is responsible for ensuring that the public or commercial data is accurate to the extent possible before including it in ICEGangs or other Federal record systems.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Automatic purge parameters permanently delete stored PII if that information has not been accessed within five years, in accordance with 28 C.F.R. Part 23. Additionally, ICEGangs users undergo agency-wide and system-specific training as described in Question 8.3.

Only DHS employees and contractors are able to directly access the ICEGangs system, which is only available through the ICE network (at DHS sites or remotely). Further, individuals cannot access ICEGangs without an account created for them by the administrator. CalDOJ users have access to a different system (CalGangs) which can query and has read-only access to ICE gang data, but do not have direct user access to ICEGangs.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

ICEGangs records containing gang members' and associates' PII are retained. General information in ICEGangs that does not necessarily pertain to a specific individual (such as estimated membership size, claimed turf, common signs, symbols etc.) is also retained.

ICEGangs does not store reports or link analyses for later review. They must be printed out in hard copy to be retained.

3.2 How long is information retained?

The gang member and associates records are stored in the system for five years after the last date they were accessed, as required under 28 C.F.R. Part 23. Records are automatically tagged when they are accessed with the expected purge date, allowing administrators to purge expired data automatically and efficiently.

Gang information that does not relate to or identify a specific person will also be purged after five years of inactivity.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

ICE is currently establishing a records retention schedule for ICEGangs records.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Retaining ICEGangs data longer than necessary would violate the Fair Information Principle of minimization which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

Mitigation: The five year period suggested for ICEGangs complements the mission requirements of ICEGangs because five years allows for sufficient time to analyze and track suspected gang members and associates, and allows for a fuller development of complicated cases where linkages between subjects, organizations, and criminal conspiracies are difficult to detect. It is also sufficiently short to reduce the risk of out-of-date information persisting indefinitely. Understanding that the retention period should not be longer than the mission and purpose of the system, five years ensures that ICE can use the

information for the stated purpose while not keeping the information longer than necessary. It should be noted that the retention period is established by 28 C.F.R. Part 23 and all users of the GangNET systems (such as CalGangs) must also comply with this retention period.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

In certain cases, select individuals within DHS who have a specific need for access may be given access to the system through user accounts on a case-by-case basis. So far, this has only occurred for U.S. Customs and Border Protection (CBP) personnel – mostly Border Patrol agents – when subjects they are encountering through border inspections or border patrol law enforcement activities meet the criteria for gang members or associates. They currently have read-only access and cannot modify ICEGangs records directly.

4.2 How is the information transmitted or disclosed?

Information is transmitted and shared with other internal organizations by directly accessing ICEGangs in the same way as standard users do – by accessing ICEGangs via the ICE Intranet via a secure DHS workstation. From there, these users have access to all the same functions and tools that ICE ICEGangs users have. However, users outside of ICE are given read-only access to prevent them from adding, modifying, or printing data.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: A risk exists that information may be shared with other DHS components without a need to know.

Mitigation: Information from ICEGangs is shared only with law enforcement organizations that have a role in the investigation of possible violations with criminal and immigrations laws. As described in Question 8 of this document, ICEGangs uses access controls and audit trails to mitigate the risk that information will be accessed by unauthorized individuals or improperly used by authorized individuals. Non-ICE users of ICEGangs currently have read-only access, which mitigates the risk that they will modify the data. All ICEGangs users undergo mandatory agency-wide and system-specific training as described in Question 8.3 which helps ensure that ICEGangs data is not shared inappropriately.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ICEGangs shares information with the CalDOJ CalGangs system for the purpose of providing information on gangs, gang members, and gang associates to the wider law enforcement community. CalGangs is a separate database based on the commercially available GangNET software that stores the same type of data found in ICEGangs.

ICEGangs and CalGangs are able to reciprocally query and access data in each other's repository. The GangNET software provides a different color scheme for each system, allowing ICEGangs and CalGangs users to visually differentiate whether they are viewing an ICEGangs or CalGangs record. Users of each system have read-only access to the data in the other system and cannot save or print the information.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Sharing with external law enforcement agencies is compatible with the purpose of the original collection, namely to improve the efficiency and effectiveness of law enforcement personnel investigating gang members and associates and gang-related activity and to facilitate sharing of gang-related information. The ICE Intelligence Records System (IIRS) SORN (DHS/ICE-006, December 9, 2008, 73 FR 74735)[2] is being amended concurrently with this PIA to include information in the ICEGangs system and to document the system's routine uses.

ICEGangs information shared with CalDOJ is done so pursuant to an existing information sharing agreement. As the community of GangNET participants grows, additional sharing partners may be identified and may give ICEGangs users access to their data and may be given access to ICEGangs data.

[2] Additional information on the ICE Intelligence Records System SORN is located at www.dhs.gov/privacy.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

A secure network connection protects the data as it flows between ICEGangs and CalGangs, owned by the CalDOJ. Users of ICEGangs and CalGangs access each other's data transparently via their own application. An Interconnection Security Agreement (ISA) between ICE and the CalDOJ is currently in progress that will establish individual and organizational security responsibilities for protection and handling of ICE Sensitive-but-Unclassified / For Official Use Only information.

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

Privacy Risk: The primary risk that results from sharing ICEGangs information with CalGangs is that CalGangs users will use ICEGangs data for purposes besides the investigation of gangs and gang-related activity.

Mitigation: External users of reciprocally supported GangNET software suites are trained, granted access, and monitored by their host agency but with training, policies and monitoring which is similar and complimentary to ICEGangs policy. Further, CalGangs users are limited to read-only access to ICEGangs and cannot print or save the information they access from ICEGangs.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

All information collected about gangs and their members and associates is law enforcement sensitive and notice is not given to the subject that a record is being created in ICEGangs. In some cases, the subject knows law enforcement is gathering information about him/her (such as information given at the time of booking or during interviews). In lieu of individual notice, this PIA and the IIRS SORN act as notice to the public that the ICEGangs system exists and that it collects information regarding gang members and associates.

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

In most cases, because of the DHS law enforcement 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? If so, how does the individual exercise the right?

In most cases, because of the DHS law enforcement purposes for which the information is collected, individuals do not have a right to consent to particular uses of the information. The information in ICEGangs will be used in accordance with this PIA and the IIRS SORN.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: A risk exists that the public is not aware of ICEGangs, or, that individuals may not be aware that their information may be contained within ICEGangs.

Mitigation: Most directly, the public is provided notice of the ICEGangs system through this PIA and the IIRS SORN. As part of this PIA and SORN process, DHS reviewed the applicable SORNs to ensure that ICEGangs is used appropriately, given the notice provided. Further, because ICEGangs is a system where many law enforcement contexts apply, notice or the opportunity to consent to use would compromise the ability of ICE to perform its 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 ICEGangs.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals may request access to records about them in ICEGangs by following the procedures outlined in the IIRS SORN (DHS/ICE-006, December 9, 2008, 73 FR 74735). All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in ICEGangs 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 also 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.

In addition to the procedures above, 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:

ICE FOIA Officer
800 North Capitol Street, N.W.

5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). 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 Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If individuals obtain access to the information in ICEGangs pursuant to the procedures outlined in the IIRS SORN, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the IIRS SORN. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, 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:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). 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 Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The procedure for submitting a request to correct information is outlined in the IIRS SORN and in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: There is a risk that an individual's record may be inaccurate and/or out-of-date.

Mitigation: ICEGangs data is never used directly as evidence to prosecute crimes. ICEGangs is solely a data repository with limited search and analytical tools that help users identify individuals and organizations that may be involved in gang-related criminal activity. It is incumbent on the investigator that uses ICEGangs to fully check all original data sources. As a safeguard, when investigating potential violations of U.S. laws ICE investigators are required to obtain and verify the original source data from the agency that collected the information to prevent inaccurate information from propagating. There is also a limited retention period for these records, and quality review checks that are performed to identify and correct records. These protections mitigate the risks posed to any individuals whose data may be in ICEGangs.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

ICE OI management is responsible for ensuring that all DHS personnel granted direct access to ICEGangs are appropriately trained and monitored. This is done by working with the ICEGangs administrator to establish user accounts as users are assigned to access ICEGangs and to update user identification, role, and access profiles as changes are needed. All users requesting access must be approved through the local ICEGangs administrator.

All ICE agents are eligible for an ICEGangs account. Some non-agents, such as ICE analysts who work on gang-related issues, have accounts as well. CBP law enforcement agents and analysts (primarily Border Patrol agents) also may have ICEGangs accounts. Other groups have access, including contractors working with ICE who are responsible for maintaining the system and contractor information technology operations and support staff. Users who access ICEGangs information from external GangNET portals are granted access through their host agency and do not have ICEGangs user accounts. All GangNET software packages with access to ICEGangs will have audit trails or access controls allowing for the tracking of information access. Each GangNET host agency is responsible for maintaining user accounts and ensuring compliance with applicable policies.

There are three access control roles that ICEGangs users might be assigned. Generally, users have read/write access so as to allow them to search and update the ICEGangs database. Some users have a limited account that allows them to search ICEGangs data, but not edit it. This role is used to ensure that individuals, such as some analysts, who do not need to edit the data, won't intentionally or inadvertently alter the ICEGangs data. Finally, administrators have full read and write access and the capacity to configure various parameters of the application. When ICEGangs access is given to CBP agents, they have read-only access and cannot modify ICEGangs records.

8.2 Will Department contractors have access to the system?

Contractors, including developers and information technology operations and maintenance staff, will have access to ICEGangs for the purpose of maintaining and upgrading the system. All contractors undergo security and background checks before being granted access and will be granted the appropriate level of access.

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

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. In addition, ICE system users must sign a "Rules of Behavior" agreement, which includes protecting sensitive information from disclosure to unauthorized individuals or groups, after passing the background investigation.

ICE will provide system-specific training to any DHS personnel who will be authorized to use ICEGangs. Training is to consist of a course of instruction that address, at a minimum:

1. The definition of a criminal street gang
2. Accepted criteria for indentifying gang members, associates, and entry of photographs
3. Criminal predicate/reasonable suspicion definitions
4. Federal, state and local law statutes and policies regarding criminal intelligence information
5. Responsibilities related to, and utilization of both the ICEGangs and CalGangs systems

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Certification and Accreditation process is in progress and is expected to be completed in March 2010.

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

Activities including subject name searches, vehicle, address, gang name, case number and contact number searches are audited. The enhanced auditing captures what new data was entered, what data existed before and after modification, and what data was deleted. In order to print from the system, a user is required to enter the purpose/reason. To comply with 28 C.F.R. Part 23, when a record is purged, all data related to that record is also purged including any audit records (i.e. the fact the record ever existing in the system has to be expunged). Security measures in place include the fact that users must be located at a government issued computer in order to access the intranet, VPN access is only granted to authorized employees and is password protected and user accounts are created on an individual basis to further secure user information.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: There is a risk that personally identifiable information in ICEGangs will be accessed inappropriately.

Mitigation: This risk 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

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The ICEGangs database is web-based commercial software tool that allows data entry and data sharing within ICE and with external law enforcement agencies. It enhances the ICE's capability to identify and investigate crimes by gang members and associates and other illegal gang-related activity.

9.2 What stage of development is the system in and what project development lifecycle was used?

ICEGangs is in the Operations and Maintenance stage of the ICE Enterprise Architecture Life Cycle Management System.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security