Privacy Impact Assessment
for

Alien Criminal Response Information Management System (ACRIMe)

April 22, 2010

Contact Point
James A. Dinkins, Director
Office of Investigations
U.S. Immigration & Customs Enforcement
(202) 732-5100

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

Abstract

The Alien Criminal Response Information Management System (ACRIMe) is an information system used by U.S. Immigration and Customs Enforcement (ICE) to support various law enforcement activities at the ICE Law Enforcement Support Center and other ICE locations. ACRIMe supports ICE's handling of and response to immigration status inquiries made by other agencies regarding individuals arrested, subject to background checks, or otherwise encountered by those agencies. ACRIMe also supports the ICE Secure Communities Program, which provides a biometric-based means to identify criminal aliens for possible removal from the United States. With the publication of this privacy impact assessment (PIA), ICE is deploying to the ICE Enterprise Network a modernized version of the ACRIMe system that provides enhanced tools for researching immigration status inquiries.

Overview

The ICE Law Enforcement Support Center (LESC) in Williston, Vermont, was originally established primarily to respond to inquiries from federal, state, local, tribal and international criminal justice agencies (i.e., law enforcement agencies, criminal courts, correctional facilities, and parole boards) regarding the immigration status of individuals they encountered while performing their law enforcement duties across the United States and internationally. ICE developed the ACRIMe system to support and keep appropriate records of these LESC activities. Since its creation, the LESC's mission and ACRIMe have expanded to support all of the customs, immigration, and law enforcement functions detailed below:

- Support the ICE Secure Communities Program, which seeks to improve public safety by implementing a comprehensive, integrated approach to identify and remove criminal aliens from the United States using biometric data;
- Respond to electronic "Immigration Alien Queries" submitted by ICE and other law enforcement and criminal justice agencies regarding the immigration status of individuals they have arrested or are investigating;
- Support "Brady Act Checks," which are background checks on foreign born persons seeking to purchase firearms in the United States;
- Create, update and clear records in the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) system about persons who are the subject of ICE-issued criminal warrants or immigration lookouts;
- Operate a 24-hour tip-line for the public to report customs and immigration violations, suspicious activity or other law enforcement matters to the Department of Homeland Security (DHS);
- Conduct immigration status checks on individuals in support of special security events; and

- Process biometric-based inquiries from the U.S. Office of Personnel Management (OPM) to determine the immigration status of federal and contract applicants and employees undergoing a background investigation.

With the publication of this PIA, ICE is initiating a phased deployment of a modernized ACRIMe system and has published in the *Federal Register* an updated system of records notice (SORN) for ACRIMe (75 FR 8377). This PIA describes Phase One of the modernized ACRIMe system, which moves the system to the ICE Enterprise Network in order to support future enhancements and to allow expanded system access to other ICE personnel outside the LESC. Phase One also enhances the ACRIMe Operations Module (discussed below) to support automated, end-to-end processing of and response to electronic Immigration Alien Queries (IAQs). This version of ACRIMe also provides greater workflow automation to assist ICE in responding to IAQs by enabling the automated query of several key immigration, customs, and criminal databases.

Deployment of Phase One ACRIMe is also intended to expand access to ACRIMe to ICE field offices, so that ICE personnel outside the LESC can assist in performing the law enforcement activities listed above. After full deployment of the modernized ACRIMe system, the legacy ACRIMe system will be retired. Future phases of ACRIMe will include automating functionality for the NCIC, Communications Center, and Tip-line Modules as well as incorporating various web services to increase overall system functionality and efficiency. These enhancements will be addressed in future updates to this PIA.

ACRIMe is divided into four separate user interfaces, called modules, (Operations Module, Communications Center Module, NCIC Section Module, and Tip-line Module) which are described below.

ACRIMe Operations Module

The ACRIMe Operations Module supports four discrete law enforcement activities in which ICE receives and responds to another agency's request for an immigration status check on an individual related to a law enforcement encounter or investigation, or a background check. The Operations Module facilitates the electronic receipt of IAQs from these agencies, and assists in the processing, research and response to the IAQs. The four law enforcement activities supported by the Operations Module are as follows:

(1) *Traditional Law Enforcement Checks* – ICE receives IAQs from federal, state, local, tribal, and international criminal justice agencies seeking the immigration status of persons encountered, arrested, in custody, or under investigation by those agencies;

(2) *Brady Act Checks* – ICE receives IAQs from the FBI (some of these originate from state law enforcement) seeking the immigration status of foreign born firearms applicants subject to a Brady Act background check to confirm they are legally in the United States before they will be authorized to purchase or possess a firearm;

(3) *Special Security Event Checks* – ICE receives IAQs from other agencies seeking the immigration status of individuals in support of special security events; and

(4) *OPM Checks* – ICE receives biometric-based IAQs from the U.S. Office of Personnel Management (OPM) seeking the immigration status of federal and contract applicants and employees undergoing a background investigation. OPM submits fingerprints to the DHS United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program for vetting against the Automated Biometric Identification System (IDENT), which are then processed via interoperability by the FBI and submitted to ACRIMe for an immigration status determination.

Generally, IAQs come to the ACRIMe Operations Module through the National Law Enforcement Telecommunications System (NLETS), which is a computer-controlled message-switching network that connects federal, state, local, and international agencies together for the purpose of information exchange.[1] Agencies submitting IAQs are seeking to know the individual's citizenship and/or immigration status. IAQs contain personally identifiable information (PII) (e.g., name, date of birth, FBI number, etc.) about the individual collected by the requesting agency.

IAQs received in the ACRIMe Operations Module are automatically assigned an ACRIMe tracking number and populated in a queue for processing by an ACRIMe user. The ACRIMe Operations Module uses personal identifiers such as name and date of birth from the IAQ to automatically search various criminal, customs, and immigration databases to gather information about the subject of the request. The search results are presented to the ACRIMe user who reviews the results and selects the most accurate and complete information to determine the individual's immigration status. As necessary, ACRIMe users have the ability to perform manual searches of other government and commercial databases during their research, and input relevant information into the ACRIMe record.

Based on the search results, the ACRIMe user prepares an Immigration Alien Response (IAR) in the system by selecting the appropriate response that communicates the individual's last known immigration or citizenship status. ACRIMe then electronically returns the IAR to the requesting agency via NLETS. For example, when an ACRIMe user determines the subject of an IAQ is a U.S. lawful permanent resident, the user will select the preset response in ACRIMe that indicates the subject is legally residing in the United States as a permanent resident. The IAR will then generate this response and send it to the requestor. The ACRIMe user can also add additional information in the remarks section of the IAR (e.g., other personal identifiers, aliases used, and last known address returned in the search results) which may benefit the requestor during their law enforcement activity. If the ACRIMe user determines the subject is an alien who may be subject to removal from the United States under the Immigration and Nationality Act (INA), an ICE agent or officer may lodge a detainer[2] via ACRIMe and the IAR is routed by ACRIMe to the local ICE field office which has local jurisdiction. For all IAQs received, ACRIMe automatically returns IARs via NLETS to the submitter of the IAQ. With limited exceptions, ACRIMe also sends a copy of the IARs to the ICE field office(s) with local jurisdiction for any appropriate follow up action and to ensure effective coordination of law enforcement activities.

---

[1] Federal law enforcement officers access NLETS either through the Department of Justice wide-area network or through the Treasury Enforcement Communications System (TECS) in order to submit IAQs. State and local law enforcement officers submit IAQs to their State Identification Bureau or authorized state agency that then transmit the IAQs electronically via NLETS to ACRIMe.

[2] An immigration detainer directs the law enforcement agency that has custody of an individual to notify ICE when

ACRIMe Communications Center Module

The ACRIMe Communications Center Module is intended to create a written record documenting calls ICE receives at the LESC (or at other ICE locations as the LESC operations are supported elsewhere) pertaining to the IAQs/IARs and to other law enforcement activities. Specifically, the Communications Center Module will document calls from IAQ submitters who have further questions regarding the response (IAR) they received from ICE, from criminal justice agencies who are contacting ICE to report a suspected customs or immigration violation, and from criminal justice agencies seeking to confirm matches against ICE-generated NCIC records (known as "NCIC Hit Confirmation" calls).

The ACRIMe Communications Center Module records may contain PII (i.e., name, phone number, etc.) about the individuals who are the subject of the call, including persons who were the subject of an IAQ/IAR, persons who are suspected of violating customs or immigration laws, and persons who are the subject of NCIC records originated by ICE. The ACRIMe Communications Center Module also retains information about the person who called ICE (typically a law enforcement officer or another government employee who is conducting or supporting a background check), any information provided by that person, what the inquiry was about, and the response provided by ICE.

After receiving a call, ACRIMe users may search ACRIMe for existing records pertaining to the subject of the inquiry, manually conduct research in various databases as necessary, and provide the results to the caller. Information provided by law enforcement officers reporting suspected customs or immigration violations is used to query various databases and generate investigatory leads, which may be referred to ICE field offices. For NCIC Hit Confirmation calls, ACRIMe users search ACRIMe for existing subject records and the ACRIMe NCIC Section Module (described below) to electronically assemble any subject information, the record entry from NCIC, and relevant criminal and immigration history, and send it in a Hit Confirmation Notification to an ICE agent for review, confirmation, and follow-up with the requesting law enforcement officer.

ACRIMe NCIC Section Module

The ACRIMe NCIC Section Module is used to create, update, and clear records in the FBI's NCIC system about persons for whom ICE has an outstanding criminal warrant or immigration lookout.[3] ACRIMe users create, update, and clear the following types of NCIC records on individuals:

- Lookout records for people who may try to re-enter the United States after being deported and those who failed to appear for deportation (previously know as "absconders"); and
- Criminal warrants for fugitives wanted by ICE for violating customs, immigration, and other criminal laws enforced by ICE.

---

the individual is about to be released so ICE can detain the individual for immigration removal proceedings.

[3] NCIC is a widely used law enforcement database that promotes information sharing about wants and warrants, criminal history, stolen property, and other law enforcement information among various federal, state, local, and tribal law enforcement personnel. Law enforcement officers in participating jurisdictions query NCIC during arrests, traffic stops, and other law enforcement encounters.

The ACRIMe NCIC Section Module maintains separate files for each NCIC record created by ICE. These files, called "hit confirmation files," provide additional information about the subject of the NCIC record and allow easy access to this information so that ICE can quickly confirm whether a person run through NCIC is in fact the person who is the subject of the active warrant or lookout. These files are maintained electronically in the ACRIMe NCIC Section Module, are automatically assigned an ACRIMe tracking number upon generation, and contain PII such as scanned images of fingerprints and photographs, information pertaining to any arrest warrants and biographical data. ACRIMe users search these files pursuant to inquiries received through the ACRIMe Communications Center Module from a law enforcement officer requesting an NCIC Hit Confirmation on an ICE-created record. ICE then informs the requesting law enforcement officer whether the person they have run through NCIC is the same person who is the subject of the ICE warrant or lookout record.

The NCIC Module is also used to enter "article" lookout records on missing, lost, or stolen firearms. When ACRIMe is modernized, article records may also include, but will not be limited to, stolen guns, badges, and radios belonging to ICE. Article records will also be entered in support of ICE investigations relating to stolen artwork or antiquities.

ACRIMe Tip-line Module

The DHS/ICE Tip-line provides a single place for the public, governmental and non-governmental organizations to report customs and immigration violations, suspicious activities or other law enforcement matters to ICE. When the general public calls the DHS/ICE Tip-line, the call is routed to an ACRIMe user who creates a written record in the ACRIMe Tip-line Module, including who placed the call (callers may remain anonymous if they wish), what the call pertains to, the information provided by the caller, when the call was received, and to which ICE office the tip was referred for action or investigation. An ACRIMe tracking number is also automatically generated for each call received and recorded in the ACRIMe Tip-line Module. The Tip-line Module records may contain personal information about the individuals who provided the tip, as well as the individuals about whom the tip was made. If enough information is provided by the caller, the ACRIMe user may manually conduct research in various government and commercial databases. Based on the findings of the search, ACRIMe users can manually create an investigatory lead in TECS and route it to the appropriate ICE field office for further investigation or action.

ACRIMe Support for the Secure Communities Program

In 2008, ICE launched the Secure Communities Program, which seeks to use information technology to identify high-risk criminal aliens and remove them from the United States.[4] The Secure Communities Program uses existing biometric databases and identification technologies to allow criminal justice agencies to perform a biometric-based federal check of criminal history and immigration status for individuals who are arrested or in custody. ACRIMe uses previously established technical capabilities between the DHS Automated Biometric Identification System (IDENT) and the Department of Justice (DOJ) FBI Integrated Automated Fingerprint Identification System (IAFIS), known as "interoperability,"

[4] For additional information, see the ICE Secure Communities Program Fact Sheet at www.ice.gov.

to automatically process biometric-based IAQs received via NLETS and return IARs to the requestor, the FBI, and appropriate ICE field offices.[5]

In a typical transaction under the Secure Communities Program, a law enforcement officer at a law enforcement agency participating in Secure Communities arrests and fingerprints an individual during the booking process. The officer electronically submits the fingerprints to IAFIS, the FBI's national fingerprint and criminal history system that provides fingerprint-based identity verification and criminal history information.[6] IAFIS determines if the individual's prints match any of its criminal history records and returns the results (including identity and criminal history information) to the officer. Additionally, the FBI automatically checks the fingerprints through IAFIS against the fingerprints stored in IDENT, a DHS biometric database that supports a broad range of DHS operations and missions. If a fingerprint match is identified in IDENT, the FBI automatically generates an IAQ on behalf of the submitting officer that is electronically sent to the ACRIMe Operations Module for processing in the manner described earlier (see the ACRIMe Operations Module section above). If no fingerprint match is identified in IDENT, no IAQ is generated and the FBI returns to the requesting law enforcement officer the appropriate response based on the IAFIS results only.

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?

The ACRIMe Operations Module gathers and maintains PII pertaining to individuals who are encountered, arrested, in custody, or under investigation by criminal justice agencies, foreign born applicants for the purchase/possession of a firearm, individuals who are the subject of a special security event check, and individuals for whom OPM is performing a background investigation. The specific information gathered and maintained varies.

The ACRIME Communications Center Module maintains PII about individuals who are the subjects of IAQs/IARs processed through the Operations Module, individuals who are reported by other criminal justice agencies for suspected customs and immigration violations, or individuals who are the subject of calls from criminal justice agencies who have received a hit in NCIC on an ICE-generated

---

[5] A more detailed explanation of the IAFIS-IDENT interoperability process can be found in the DHS PIA *United States Visitor and Immigration Status Indicator Technology (US-VISIT) Program for the First Phase of the Initial Operating Capability of Interoperability between DHS and the U.S. Department of Justice* (Oct. 28, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_phase1ioc.pdf

[6] *See* U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Integrated Automatic Fingerprint Identification System (IAFIS) Privacy Act System of Records Notice, JUSTICE/FBI-009, October 30, 2006, 64 FR 52347.

record. PII maintained in the Communications Center Module varies depending on the information provided by the caller, but may include any/all of the information maintained in the Operations Module described above. The Communications Center Module also allows ACRIMe users to search and view existing records and information maintained in the Operations and NCIC Section Modules, in order to assist callers in resolving questions about IAQs/IARs and NCIC hits.

The ACRIMe NCIC Section Module collects and maintains PII about persons of interest to ICE due to criminal, customs, or immigration violations. Specifically, the NCIC Section Module maintains records about individuals for whom ICE has created an immigration lookout record in NCIC (those who may try to re-enter the United States after removal and those who have failed to appear for removal), and individuals who are the subjects of criminal warrants and who are wanted by ICE for violations of federal criminal laws. The NCIC Section Module maintains biographic information about the subject of an ICE-generated NCIC record.

Finally, the ACRIMe Tip-line Module maintains PII about members of the public who contact the DHS/ICE Tip-line to report suspected immigration, customs, or criminal violations, suspicious activities or other law enforcement matters. Information collected and maintained in the ACRIMe Tip-line Module can vary.

ACRIMe also generates standard and ad hoc statistical and performance-based reports using workflow information maintained in ACRIMe to help manage the LESC workload and comply with various reporting requirements (e.g., Congressional and senior management). Examples include fiscal year activity and daily IAQ processing reports as well as reports reflecting the number of IAQs processed as part of the Secure Communities Program.

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

Information in the ACRIMe Operations Module is obtained from ICE and other agencies that have collected the information directly from the individual. Criminal justice agencies, and agencies that conduct background or special security event checks, collect information from the individual during the course of a law enforcement encounter (such as an arrest or an ongoing investigation) or from forms completed by an individual (such as a firearms application or employment application). Some of that information may be passed to ICE in the IAQ.

Information in the Communications Center Module is obtained from law enforcement agencies or other agencies submitting IAQs in the event they are seeking additional information about an IAR. Information in this Module is also received from law enforcement agencies that contact ICE to report suspected customs and immigration violations or for an NCIC Hit Confirmation. Information in the NCIC Section Module is obtained from ICE agents and officers who collect this information during the course of ICE criminal investigations and customs and immigration enforcement activities. Information in the Tip-line Module is obtained from members of the public, governmental and non-governmental organizations, who phone in tips about customs and immigration violations, suspicious activities or other law enforcement matters.

While conducting research for inquiries received from other agencies and tips from members of the public, ICE personnel obtain information from various sources that may be input into ACRIMe in order to determine a person's immigration status, resolve an NCIC hit, or determine if a tip is an actionable lead.

ACRIMe itself is the source of reporting generated by the system.

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

The information in ACRIMe is collected and maintained in order to support ICE's efforts to enforce U.S. customs and immigration laws. This may include, but is not limited to, improving and modernizing efforts to identify aliens who may be removable under U.S. immigration laws because they have been convicted of a crime. ACRIMe information is also used to allow other agencies to obtain from ICE real-time immigration status information about an individual, and allow criminal justice agencies to confirm hits against ICE-generated NCIC records. Finally, the information collected in ACRIMe facilitates ICE's collection of tips on suspected violations of customs and immigration laws from the public and other government agencies.

1.4 How is the information collected?

With the exception of tips received by the Tip-line, ICE does not collect information stored in ACRIMe directly from individuals. Most information is collected by the agencies contacting ICE from individuals (e.g., during law enforcement encounters such as an arrest or investigation) or from forms completed by the individual (e.g., federal background check and employment forms, firearms application forms). In some cases, information about an individual's identity or activities may be obtained from third parties who have observed the information and believe it is suspicious (e.g., tips phoned in by the public).

Information received through the ACRIMe Operations Module arrives electronically in the form of IAQs via NLETS. Information in the ACRIMe Communications Center Module and the Tip-line Module is collected telephonically from callers. The NCIC Section Module information is collected via e-mail from ICE agents and officers. Finally, ICE collects information from the various government and commercial databases listed in Question 1.2 above either through manual query or through an electronic interface in ACRIMe that automatically queries the databases using personal identifiers in the IAQ.

1.5 How will the information be checked for accuracy?

IARs are reviewed by ICE supervisors and dedicated quality assurance staff for quality and accuracy after being returned to the submitter of the IAQ. The quality assurance staff randomly select up to 5 percent of completed IAQs for review. Quality assurance personnel review processed IAQs to ensure the ACRIMe users arrived at the correct immigration status determination based on the information automatically gathered through ACRIMe. Although ACRIMe provides automated search capabilities of various government databases, the IAQ process requires an ACRIMe user to manually review query results and make the immigration status determination. The ACRIMe user can view the

original record queried in the ACRIMe Operations Module to examine the full context and content of the record, which also increases the likelihood that data errors will be identified. For manual searches conducted by ACRIMe users based on IAQs received in the Operations Module or calls or tips recorded via the Communications Center and Tip-line Modules, ACRIMe users follow standard operating procedures and written search protocols when conducting searches to ensure consistency and accuracy of immigration status determinations across all ACRIMe users. The information recorded in the Communications Center and Tip-line Modules is also verified against the data gathered from the other sources that are searched. In addition, IAR recipients can manually compare the identifying data submitted in the original IAQ against the information in the IAR to ensure the response pertains to the same individual.

In the ACRIMe NCIC Section Module, all ICE-generated NCIC records are verified by a second ACRIMe user after the record is created in NCIC. There is also a subsequent review of all ICE-generated NCIC records 90 days after entry as well as annually, at which time the accuracy of the information is validated and the status of the warrant or lookout is confirmed. Additionally, when ICE receives a call on an ICE-generated NCIC record, an ICE employee will confirm if the warrant or lookout record is still valid and will assist the locating agency in determining if the subject in custody or under investigation is the same person identified in the ICE-generated NCIC record.

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

Authority for maintenance of the system is provided in Section 504 of the Immigration and Nationality Act of 1990 (Public Law 101-649); 8 U.S.C. §§ 1103, 1324(b)(3), 1360(b); the Brady Handgun Violence Prevention Act (Brady Act) of 1993, Public Law 103-159 (18 U.S.C. § 922(d)(5) and (g)(5)), FY2008 DHS Appropriations Act (Public Law 108-161, 1844, 2050 (2007)); Immigration and Nationality Act (INA) provisions regarding removal of criminal aliens (INA §237(2) and §238); and the Economy Act (31 USC § 1535).

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: There is a risk of unauthorized access to or disclosure of information contained in ACRIMe.

Mitigation: This is mitigated by user training, the maintenance of secure passwords, and the practice of operational and informational security. Individuals who are found to have accessed or used the ACRIMe system in an unauthorized manner will be disciplined in accordance with ICE policy. ICE components are ultimately responsible for ensuring the data is used appropriately. This is done by the establishment of standard operating procedures that stipulate proscribed and permitted activities and uses, and integrity controls. Additionally, ACRIMe users return a limited amount of data in IARs that is narrowly tailored to information that is useful to the law enforcement purpose for which the data was requested. Any information provided via the telephone to law enforcement officers is limited to those

officers with authorization to request the information and who have been verified and authenticated by an ACRIMe user.

Privacy Risk: There is a risk of creating an inaccurate record of identity about an individual encountered by a criminal justice agency based on the information selected by the ACRIMe user to prepare an IAR.

Mitigation: This risk is mitigated by user training which stresses the importance of making accurate immigration status determinations, and by the use of standard operating procedures that require quality assurance and accuracy checks by designated quality assurance and supervisory personnel.

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.

The ACRIMe Operations and Communications Center Modules use personal information about individuals to support the Secure Communities Program and to provide criminal justice agencies and officers real-time immigration status determinations about arrested or encountered individuals and individuals who are the subject of ongoing investigations. This information is also used to support the screening of foreign born applicants for firearms (Brady Act Checks), special security event checks, and OPM checks. Specific to supporting the Secure Communities Program as described in the Overview, fingerprints collected from an arrested or encountered individual are used to query the entire population of records maintained in IDENT and IAFIS to better identify (with greater accuracy) the subject of the inquiry as well as identify adverse criminal data that may make the individual removable from the United States. Using identifying information submitted in an IAQ, ACRIMe automatically searches government databases to retrieve the available information about the IAQ subject in order to assist the ACRIMe user in making an immigration status determination. This same PII is also used to manually query government and sometimes commercial databases for the same purpose. Many databases, such as the NCIC criminal history files, contain SSNs which allow ACRIMe users to improve the accuracy of the identification of the subjects. The immigration status determinations made by ICE are used by the submitter of the IAQ to make determinations about the course of a law enforcement action, a firearms or federal employment application, or an individual who is seeking access to, or is otherwise involved in, a special security event. Certain immigration status determinations may also be used by ICE field offices in deciding whether to issue an immigration detainer for an individual who may be in violation of U.S. immigration laws.

The information in the ACRIMe NCIC Section Module is also used to help respond to NCIC Hit Confirmation calls (on ICE-generated NCIC records) phoned in by law enforcement officers – specifically, to determine if the subject of the NCIC query is the same person who is the subject of ICE's NCIC record – and provide supplemental information about the individual so that appropriate follow up

action can be determined (e.g., arresting the individual on a criminal warrant or detaining an individual who is removable for immigration violations).

The information in the ACRIMe Communications Center Module is used to document tips received from ICE and other criminal justice agencies, and calls related to NCIC hits on ICE-generated NCIC records. Personal identifiers received from callers to the ACRIMe Communications Center or Tip-line Modules are used to manually search existing records in ACRIMe and various government and commercial databases to identify the subject of an IAR, NCIC Hit Confirmation call or tip. Information provided by law enforcement officers reporting suspected customs or immigration violations is used to query various databases and generate investigatory leads for further action. Law enforcement officers use information provided from ACRIMe to better identify encountered individuals, determine their immigration status, and determine if they are wanted for any suspected criminal activity. NCIC Hit Confirmation calls received by the ACRIMe Communications Center Module use information provided by the requesting law enforcement officer such as the name and A-Number of the individual suspected of being the subject of a criminal arrest warrant or immigration lookout to search ACRIMe for prior subject records and the NCIC Section Module for existing ICE-generated NCIC records. Information recorded in the ACRIMe Communications Center Module such as the requesting law enforcement officer's name, phone number and the IAR in question is used to provide adequate follow-up and clarification of information already processed in the ACRIMe Operations Module and returned in an IAR.

Information recorded in the Tip-line Module provided from members of the public, governmental and non-governmental organizations who contact the DHS/ICE Tip-line such as the name and address about the individual(s) on whom the tip is made, is used to track, evaluate, and respond to reports of suspicious activity or suspected illegal activity, to generate investigatory leads for the local ICE office that may investigate the tip, and for the eventual prosecution of illegal activity.

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

ACRIMe supports the automated search of various government law enforcement, border, visa, and immigration databases based on personal identifiers. The system returns matching results to the user, who is trained to analyze this data and other data gathered manually from other databases to make an immigration status determination. The system does not conduct any analysis beyond the search for matching records. ACRIMe does not perform these searches but sends the queries to the destination databases, which perform the search using whatever query tools are standard for that system. ICE does not limit the searches to only those personal identifiers provided in the IAQ. Additional personal identifiers discovered during the research process may be used to refine subsequent searches and some searches may be re-generated using the additional personal identifiers discovered by the ACRIMe user.

ACRIMe also generates standard and ad hoc statistical and performance-based reports using workflow information maintained in ACRIMe to help manage the LESC workload and comply with various reporting requirements (e.g., Congressional and senior management).

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

ACRIMe users may manually query commercial databases to gather additional information on persons suspected of illegal activity pursuant to calls received by the Communications Center and Tip-line Modules and inquiries processed through the NCIC Section Module. Any relevant information may be provided to a law enforcement officer submitting a request telephonically via the ACRIMe Communications Center Module. This information may also be used to further substantiate investigatory leads created in TECS which are then forwarded to an ICE field office for appropriate action.

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.

Privacy Risk: There is a risk that PII will be accessed by unauthorized individuals or for unauthorized purposes.

Mitigation: ACRIMe employs security and access controls as well as auditing processes to mitigate this risk. Access to ACRIMe is limited to authorized ICE users, and the system maintains audit logs based on user IDs and ACRIMe tracking numbers that are reviewed to ensure appropriate use of information and system integrity. Additionally, users also receive computer security and privacy awareness training to mitigate the risk that information will be used inappropriately.

Privacy Risk: There are several risks associated with the use of multiple databases from DHS, other governmental and commercial entities, which contain information on all types of individuals, including U.S. Citizens.

Mitigation: These risks are mitigated by leveraging the knowledge and experience of ACRIMe users and ICE agents who are trained to exercise experience, discretion and judgment, while searching and cross checking information from multiple databases. These procedures ensure the highest level of accuracy in the collection and dissemination of data provided to the end user.

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?

All information entered into and gathered by the various ACRIMe modules as described above is retained by the system, including subject information provided in IAQs and IARs, ICE-generated NCIC hit confirmation files, communication center and Tip-line information.

3.2 How long is information retained?

DHS proposes to maintain the IAQ and IAR records pertaining to traditional law enforcement checks for seventy-five (75) years and Brady Act, special security event and OPM checks for five (5) years from the date an immigration status determination is made and IAR returned, after which the records will be deleted from the ACRIMe system. DHS proposes to maintain NCIC Module records (containing the underlying basis for the ICE-generated NCIC record) for 75 years from the date the record is removed from NCIC. DHS proposes to maintain Communication Center Module records containing NCIC Hit Confirmation calls for 75 years and follow-up calls to IARs for the time period consistent with the type of query conducted. Additionally, DHS proposes to maintain suspicious activity reporting in the Tip-line and the Communications Center Modules for ten (10) years from the date of the tip.

The 75 year retention periods are consistent with the U.S. Government's policy to retain records related to immigration, law enforcement, and law enforcement intelligence for the approximate lifetime of an individual.

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

ICE is developing a proposed retention schedule consistent with the retention periods described above for submission to NARA.

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: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in ACRIMe is retained for the timeframes outlined in Question 3.2 to allow ICE to determine the immigration status of an encountered individual based on the most accurate and comprehensive information available as well as facilitate effective information sharing and coordination throughout the law enforcement community. The retention period is also consistent with general law enforcement system retention schedules and is appropriate given ICE's mission and the importance of the law enforcement data pertaining to customs, immigration and other violations.

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?

Access to ACRIMe is currently limited to authorized ICE users, but information is routinely shared with other DHS components, such as the U.S. Secret Service, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, U.S. Coast Guard, and the Transportation Security Administration, in furtherance of their missions or based upon inquiries they submit to ICE. Typically, information is shared with other internal DHS organizations through the same IAQ/IAR process described above or by telephone.

Information shared with DHS components may include all of the available information that resides in the ACRIMe system. This could include IARs, NCIC hit confirmations, or suspicious activity reporting.

4.2 How is the information transmitted or disclosed?

IARs are transmitted to the requestor and retrieved by the requestor via NLETS. DHS users may access NLETS through TECS or other computer systems that interface directly with NLETS.

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: There is a risk of unauthorized or improper dissemination of data contained in the ACRIMe system.

Mitigation: This is mitigated by limiting system access to only authorized ICE users. The risk is also mitigated by training, the maintenance of secure passwords, and the practice of operational and informational security. Individuals who are found to have accessed or used the ACRIMe system in an unauthorized manner will be disciplined in accordance with ICE policy. DHS components that receive information from ACRIMe are ultimately responsible for ensuring the data is used appropriately. This is done by the establishment of standard operating procedures that stipulate proscribed and permitted activities and uses, and integrity controls. Transmission of ACRIMe data to other DHS components is done through secure means and in accordance with DHS policies on safeguarding Sensitive PII.

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, Local and Tribal government, and the private sector.

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

ICE may share the results of its immigration status determinations with the submitters of IAQs, which include criminal justice agencies, and agencies conducting Brady Act Checks, OPM checks, and special security event checks. This information is shared to allow those agencies to take appropriate follow up action upon learning the individual's immigration status, which may include denial of a firearm, employment, or access request. For IAQs and IARs processed under the Secure Communities Program and IAQs submitted by OPM, this data is passed through the FBI's technological infrastructure, therefore, this information is also shared with the FBI.

In addition, the Government of Canada may submit IAQs for processing through ACRIMe and receive IARs. Currently, criminal justice agencies in Canada have access to NLETS and are able to leverage ACRIMe capabilities for immigration and law enforcement purposes. Information is shared with Canadian criminal justice authorities pursuant to existing information sharing agreements and understandings between Canada and the United States. U.S. immigration status information may be useful to Canadian authorities to assist them in verifying an individual is a U.S. citizen or resident, or determining whether the individual has a criminal history in the U.S. that may be relevant to their ability to remain in Canada pursuant to relevant Canadian border and immigration laws.

ACRIMe shares information with the FBI when generating warrants in NCIC to include other biographical data about the subject of the warrant. ICE also shares information pertaining to its NCIC records with criminal justice agencies that query NCIC and match against the ICE-generated NCIC record. ICE will notify that agency whether the subject of the query is the same person who is the subject of the NCIC record, and if so, the basis for the NCIC record (e.g., criminal violations for which the individual is wanted). The criminal justice agency will use that information to decide on any appropriate follow up actions, e.g., arrest of an individual who is the subject of an ICE criminal warrant. The ACRIMe System of Records Notice (SORN) contains a complete list of routine uses which describe the various purposes for which ACRIMe information may be shared outside DHS.

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.

Yes. In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as shown in the ACRIMe SORN (DHS/ICE-007, February 24, 2010, 75 FR 8377) published in the *Federal Register*.

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

ACRIMe information provided in IARs is shared externally using NLETS, a secure sharing system dedicated to the entire justice community. NLETS uses an advanced encryption method, which allows for identification of users and devices, and comports with the FBI's Criminal Justice Information Services NCIC Security Policy.

ACRIMe users are able to create and update a warrant in the FBI's NCIC system through an established interconnection between NCIC and ACRIMe, which ensures any biographical subject data transmitted to NCIC is appropriately safeguarded in accordance with the DHS and ICE network security provisions and the NCIC Security Policy.

IAQs are also checked against INTERPOL data via a computer interface between ACRIMe and NLETS and are submitted to the U.S. National Central Bureau (USNCB) to receive a positive or negative response against the INTERPOL data. If a positive result is received, a copy of the IAR is sent via NLETS to the USNCB office in Washington, D.C. and to the responsible ICE field office for any follow up action deemed appropriate.

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

Privacy Risk: There is a privacy risk of unauthorized or improper dissemination of data contained in the ACRIMe system.

Mitigation: Records in ACRIMe are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to ACRIMe is limited to authorized ICE users who are assigned unique user IDs and an ACRIMe tracking number. The external sharing of information is based on an established need to know, and any information shared is transmitted either electronically via NLETS. Additionally, the ACRIMe system employs a real-time auditing function that records all transactions conducted by authorized users based on user IDs and ACRIMe tracking numbers.

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?

General notice of information collected in the system is provided by this PIA and the updated ACRIMe SORN. Callers to the DHS/ICE Tip-line are notified orally that information given will be forwarded to the local ICE office for investigation, as appropriate. For persons who are applying for firearms licenses or federal employment, the agencies that collect the information provide written notices on forms that the applicants complete stating that their information will be used for background check purposes.

For the other information collected in ACRIMe, because of the law enforcement and customs and immigration purposes for which the information is collected, opportunities for the individual to be notified prior to the collection of information may be limited or nonexistent. Individuals may be notified by other law enforcement agencies at the point of collection of the original data that their information may be shared for law enforcement purposes. Because ICE does not directly collect most of the information gathered by ACRIMe, ICE is also not in the best position to provide individuals notice prior to the collection of information.

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

Callers to the DHS/ICE Tip-line are asked if they would like to remain anonymous. If they request anonymity, it is noted in the call record. Information provided on the DHS/ICE Tip-line is purely voluntary. For persons applying for firearms licenses or undergoing OPM background checks, the provision of certain information may be mandatory in order to obtain the benefit they are seeking. Those determinations are made by the agencies that collect the information from the individuals and notice of the voluntary nature of any information requested is provided to these individuals in the notice referenced in Question 6.1 above, as required by applicable federal and state laws. For the other information collected in ACRIMe, in most cases, because of the law enforcement and immigration purposes for which the information is collected, opportunities to decline are 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?

Individuals who call the DHS/ICE Tip-line have the option to remain anonymous, but are not afforded the right to consent to how information provided will be used. Individuals who are the subjects of Brady Act, special event, and OPM checks may have been asked to sign consent forms authorizing the collection of information from agencies, individuals, and organizations for the purpose of performing the background checks. For the other information collected in ACRIMe, because of the law enforcement and immigration purposes for which the information is collected, no such consent exists. Because ICE does not directly collect most of the information gathered by ACRIMe, ICE is not in the best position to provide individuals an opportunity to consent to particular uses of the information.

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: There is a risk that individuals may not be aware their information may be contained within the ACRIMe system.

Mitigation: The risk is mitigated primarily by the public notice provided through this PIA and the updated ACRIMe SORN. Notice is also given verbally over the phone to individuals who call the DHS/ICE Tip-line. They are notified by the responding ACRIMe user at the time of the call that the information provided will be forwarded to the appropriate local ICE field office. Individuals may be notified at the point of collection of the original data that their information may be shared for law enforcement purposes. Additional notice may be limited or nonexistent because providing such notice could compromise the underlying law enforcement purpose of the system and may put ongoing investigations at risk.

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 ACRIMe by following the procedures outlined in the ACRIMe SORN. 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 ACRIMe 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 the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). 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, SW, Building 410, STOP-0550, Washington, DC 20528.

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

If individuals obtain access to the information in ACRIMe pursuant to the procedures outlined in the ACRIMe 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 ACRIMe 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 the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). 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, SW, Building 410, STOP-0550, Washington, DC 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 ACRIMe 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?

If an individual is not satisfied with the response to an access or correction request, he or she can appeal to the appropriate authority provided for in the FOIA process. The individual will be informed how to file an appeal if and when a request is denied. In addition, if any actions are taken against the individual as a result of or in connection with information requested or provided through ACRIMe, certain statutory or regulatory appeal rights or constitutional due process rights to access, amend, or otherwise challenge the information may exist. For example, if an individual is arrested as a result of the existence of an ICE-generated NCIC record indicating a criminal warrant exists, the individual may have statutory or constitutional rights to challenge the arrest and access information concerning the validity or basis for the warrant. Individuals who are delayed or denied a firearm during the Brady check process may have rights to appeal the delay or denial under the relevant DOJ regulations at 28 CFR Part 25.10.

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

Individuals can request access to information about them through the FOIA process and may also request that their information be corrected. The nature of ACRIMe and the data it 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 the records in ACRIMe are collected from various other databases within DHS components and offices as well as other federal, state, local, and international agencies and commercial databases, individuals may also have the option to seek access to and correction of their data directly from the agencies or organizations which originally collected it. Information that is corrected in the original data source can only be updated in ACRIMe when the information is again accessed in the source database or based upon a request of an individual, or when ICE becomes aware of inaccuracies of the information.

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?

Each user account is assigned certain roles. Each of these roles has a set of privileges defined for it to ensure overall system integrity. The ACRIMe system administrator can elect to assign all the privileges for a given role or can select only certain privileges to assign. Access is limited to ICE personnel who have a need to access the system based on their roles in support of law enforcement activities, or the administration of immigration laws and other laws administered or enforced by DHS. The ACRIMe user roles are as follows:

- Specialist – Respond to queries, create/update warrants, and answer Tip-line calls
- Agent – Create detainers, verify hit confirmations, and review IARs
- Supervisor – Track and report productivity and specialist performance, management reporting, and assign roles
- Section Chief – Track and report productivity and specialist performance
- Quality Assurance Specialist – Conduct quality assurance checks on query responses and generate critical error reports
- Technical Support – System maintenance and upgrades, Help Desk support, and implement enhancements
- Administration – Create reports

These user roles are consistent across all modules of ACRIMe. Access roles are assigned by a supervisor based on the user's job and assignments, and implemented by an administrator. Access roles are reviewed regularly to ensure users have the appropriate access. Individuals who no longer require access are removed from the access list. The system administrator establishes user accounts and updates user identification, role, and access profiles as changes are needed. Access is audited and the audit logs are reviewed on a regular basis.

8.2 Will Department contractors have access to the system?

Yes. Information technology (IT) contractors supporting ACRIMe have access to perform IT development, operations and maintenance tasks on the system. All contractors undergo an extensive background investigation prior to accessing ACRIMe. No other contractors currently have access to the system.

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 trainings, specifically the Culture of Privacy Awareness and the Information Assurance Awareness Training. Additionally, ACRIMe users are required to complete the Integrity Awareness Program training, NCIC certification (every two years), and the TECS Privacy Awareness Certification Course (every two years).

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

The legacy ACRIMe system was awarded its Authority to Operate (ATO) on September 24, 2008. The modernized ACRIMe system is currently undergoing a new Certification and Accreditation, which is expected to conclude in April 2010.

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

Technical controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The ACRIMe system ensures each user is authenticated before access is permitted. Each user must be approved to access ACRIMe modules prior to accessing the system. The ACRIMe system utilizes unique user IDs and passwords. In addition, the user is assigned a role, which governs the user's access rights. User roles are determined by their work assignment and whether or not they have a supervisory role. The user ID and password are used for user authentication and identification.

The ACRIMe system uses a real-time auditing function which records all ACRIMe system activity to include, but not limited to, the transmission of data to and from the NCIC and NLETS systems, user activity based on user IDs and ACRIMe tracking numbers, databases searched and results returned, and the determination made. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. ICE reviews audit trails when there is indication of system misuse and at random to ensure users are accessing and updating records according to their job function and responsibilities.

All failed logon attempts are recorded in an audit log and periodically reviewed. The ACRIMe Information System Security Officer will review audit trails at least once per week, or in accordance with the System Security Plan. The ACRIMe system and supporting infrastructure audit logs will be maintained as part of and in accordance with the existing ICE system maintenance policies and procedures. 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 to the ICE Office of Professional Responsibility.

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: The risk is unauthorized or improper dissemination of data contained within the ACRIMe system.

Mitigation: This is mitigated by training, the maintenance of secure passwords, and the practice of operational and informational security. Individuals who are found to have accessed or used the ACRIME system in an unauthorized manner will be disciplined in accordance with ICE policy. DHS components are ultimately responsible for ensuring that the data is used appropriately. This is done by the establishment of standard operating procedures that stipulate proscribed and permitted activities and uses, and integrity controls.

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?

ACRIMe is a system modernization project converting the original ACRIMe database into a web-based, integrated common interface system on the ICE Enterprise Network.

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

ACRIMe is in the development phase of the system lifecycle. ACRIMe Phase One is scheduled for testing in March 2010 and deployment by April 30, 2010.

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

No.

Responsible Official

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

Approval Signature Page

Original copy signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security