



Privacy Impact Assessment  
for the

# Fugitive Case Management System (FCMS)

August 11, 2009

**Contact Point**

**David Venturella**

**Acting Director, Detention and Removal Operations**

**U.S. Immigration and Customs Enforcement**

**(202) 732-3100**

**Reviewing Official**

**Mary Ellen Callahan**

**Chief Privacy Officer**

**Department of Homeland Security**

**(703) 235-0780**



## Abstract

The Fugitive Case Management System (FCMS) is a case management database owned by U.S. Immigration and Customs Enforcement (ICE) that processes, tracks, and stores information about aliens who fail to leave the United States after receiving a final order of removal, deportation or exclusion, or who failed to report to ICE after receiving notice to do so (i.e., fugitive aliens). FCMS supports the ICE National Fugitive Operations Program, which is intended to locate, arrest, and remove fugitive aliens from the United States. ICE has prepared this Privacy Impact Assessment (PIA) because the system collects personally identifiable information (PII).

## Overview

FCMS is owned and maintained by ICE's Office of Detention and Removal Operations (DRO), Fugitive Operations Support Center (FOSC), whose mission is to promote public safety and national security by ensuring the departure from the United States of all removable aliens through the fair and effective enforcement of the nation's immigration laws. FCMS tracks and stores information that assists in the location and arrest of fugitive aliens. FCMS was first launched in June 2006 and is undergoing a conceptual and architectural upgrade. The new version of FCMS will be deployed in August 2009. The information stored in the current version of FCMS will transfer to the new version of FCMS. This PIA describes the functionality of and data maintained in the new version of FCMS.

### Background

Generally, fugitive aliens are aliens who fail to leave the United States after receiving a final order of removal, deportation or exclusion, or who fail to report to ICE after receiving notice to do so. ICE established the National Fugitive Operations Program in 2003 pursuant to a Congressional mandate to significantly reduce the fugitive alien backlog. In addition to locating, arresting, and removing fugitive aliens, the program also seeks to identify aliens who are no longer fugitives because they have left the country voluntarily, successfully adjusted their immigration status, or are currently incarcerated somewhere in the United States. Under this program, ICE established Fugitive Operations Teams consisting of DRO Officers specifically assigned to investigate fugitive alien matters. The Fugitive Operations Team members work with other law enforcement agencies using law enforcement analytical and investigative information to locate and arrest fugitive aliens. Based on an established priority scoring system, the Fugitive Operations Teams prioritize enforcement efforts on fugitive aliens who pose a threat to national security and community safety such as members of transnational street gangs, child sex offenders, and aliens with prior convictions for violent crimes.

DRO Officers use FCMS to track fugitive aliens actively being sought for arrest and removal from the United States. FCMS is also used to identify, track, and manage "leads" (i.e., tips or other information) that may help locate fugitive aliens. These leads may consist of new information (such as new addresses) gathered from public or government records, or information from Federal and state correctional facilities that may locate a fugitive alien now in jail or prison. The leads are either entered into FCMS manually on a record-by-record basis by DRO Officers in the field or uploaded from extracts of other government and commercial data systems by DRO Headquarters staff. The new leads are either assigned manually by



members of the National Fugitive Operations Program, or sent by FCMS based on zip code of the address provided by the alien to the Fugitive Operations Teams with official jurisdiction to investigate and, where possible, arrest fugitive aliens. The DRO Officers on the Fugitive Operations Teams update FCMS with information about what actions they are taking to follow up on fugitive alien leads. Once a fugitive is arrested, DRO Officers document the arrest information and update the fugitive alien's status in FCMS to reflect that the fugitive is in custody. In the course of arresting fugitive aliens, DRO Officers may also encounter and arrest other illegal aliens. The identity and immigration status of the non-fugitive aliens are verified through information in federal databases, interviews, and fingerprint checks prior to entering the encounter as an arrest of an illegal alien in FCMS. FCMS information about non-fugitive arrests is used solely for the purpose of reporting arrest statistics for the National Fugitive Operations Program.

FCMS maintains biographical, immigration case history, criminal history and/or arrest information related to the fugitive alien population. FCMS also receives information from other DHS systems such as ICE's Enforcement Integrated Database which may be used to update fugitive alien information in FCMS. The information from such systems includes immigration case history, criminal history and biographical information on fugitive aliens. The information on fugitive aliens is used to secure their arrest and removal from the United States. FCMS also maintains a limited amount of information about DRO users, such as names, position titles, geographical work location and office telephone numbers.

FCMS is comprised of three major user interfaces: Leads, Activities, and User Menus. The Leads Menu is used by Fugitive Operations Teams and the FOOSC to forward information from DRO-HQ to a DRO field office about possible addresses or other leads that may help locate a fugitive alien. The Activities Menu is used to process information that shows what actions have been taken by the Fugitive Operations Team to follow up on a particular lead, including the biographical information of the fugitive alien. The User Menu tracks the users and subsystem access permissions within FCMS. User access to FCMS is limited to DRO employees on Fugitive Operations Teams and those assigned to work for or oversee the National Fugitive Operations Program.

#### *Typical Transaction*

In a typical FCMS transaction, new leads on fugitive aliens are identified by ICE, such as new address information gathered from public or government records; information from Federal and state correctional facilities that may locate a fugitive alien in jail or prison; or the recent location of a fugitive alien from parole or probation data. These leads are entered manually into FCMS on a record-by-record basis by DRO Headquarters and Field Officers or uploaded from extracts of other DHS, government and commercial systems by DRO Headquarters Officers.

Once the lead information is manually or electronically populated into the FCMS database, these new leads are assigned to the appropriate Fugitive Operations Team that has the corresponding geographical jurisdiction. The receiving team investigates the lead information, and pursues the arrest of the fugitive. As part of the investigative process, the DRO Officers on the Fugitive Operations Team will evaluate the various lead and address information, manually compare sources of information such as leads from commercial sources against federal government databases, validate information for accuracy, and document and update FCMS as the investigation progresses. If the fugitive is arrested, the DRO Field Officer updates the fugitive alien's status in FCMS to reflect he/she is now in ICE custody.



## 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?

FCMS consists of biographical, lead, and arrest data which facilitates the identification and removal of fugitive aliens from the United States. The information that is collected, used, disseminated and maintained in FCMS consists of the following:

- Fugitive alien information, to include:
  - Biographical: Name, aliases, place and date of birth, Social Security number (SSN), Alien Number (A-Number), sex, gang affiliations (if any) and possible U.S. addresses.
  - Immigration Case History: Date of last known U.S. entry, place of last U.S. entry, removal charges, entry class, prior DHS apprehension date(s), removal case category, docket case office, Treasury Enforcement Communications System (TECS) Number (if any), and ICE custody date.
  - Criminal History: FBI number, Fingerprint Identification Number (FIN), mug shots, State Identification (SID) number, summary of conviction(s), and conviction date(s).
- Non-fugitive alien information, concerning non-fugitive illegal aliens arrested during Fugitive Operation Team activities. This information is limited to the A-Number and date and location of the arrest. The information is only collected as a statistical record of the arrest of an illegal alien who is a non-fugitive at the time of arrest and not to track the immigration history of the alien. The non-fugitive alien information is not updated to reflect a change in immigration status, i.e., change from non-fugitive alien to fugitive alien or from non-fugitive alien to a U.S. citizen. Any change of immigration status is reflected in other immigration-related systems.
- Activity (Officer) information, to include type of action (e.g., arrest, surveillance, etc.); name, title, and field office of the officer; action location; operation name (if any); address of location where and date when a fugitive or illegal alien is arrested; any notes that the officer inputs regarding the case (e.g., checks run, addresses checked, etc.) .
- Lead information, to include lead number; information about the source of the lead (agency, officer name, etc.); DRO Field Office point of contact and other information on referral of the lead to the field; and lead notes, which vary but generally contain information concerning possible addresses for the fugitive alien and systems checks performed by DRO Officers.

FCMS also consists of a reporting tool that compiles statistical information to generate various reports for investigative and program analysis. Leads Reports provide the number of total leads, the number of leads closed, and the percentage of leads closed for every field office during a designated period of time. Total Fugitive and Non-Fugitive Enforcement Activity Reports provide the number of fugitive



(criminal and non-criminal) and non-fugitive (criminal and non-criminal) arrests and the number of fugitive and non-fugitive removals for each Field Office during a designated time period. These reports do not contain PII and are used for statistical purposes only.

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

ICE obtains fugitive alien information from ICE systems; public or government records; Federal and State correctional facilities that may locate a fugitive alien in jail or prison; other DHS and government systems that contain information about the alien as the result of immigration enforcement or other law enforcement encounters with the alien; records of the alien's admission into the U.S; and commercial data aggregators. Additionally, information can also be collected directly from the alien at the time of arrest and/or placement into ICE custody, and from the DRO Officers during the arrest activities. The specific sources of the information collected, used, disseminated and maintained in FCMS are as follows:

Fugitive alien information may be obtained from the alien at the time of arrest and/or placement into ICE custody, as well as from ICE's Enforcement Integrated Database (EID), Removable Alien Records System (RARS) System of Records, (DHS/ICE-011, May 5, 2009, 74 FR 20719), other Federal systems of records, and other sources.

Non-fugitive alien information is obtained from the alien at the time of arrest and/or placement into ICE custody, and EID.

Activity information is obtained from DRO Field Officers manually inputting information obtained from directly performing the activity related to tracking leads, or locating and arresting a fugitive.

Lead information is obtained from the following sources:

- DRO Field Officers manually inputting information based on their evaluation of the various lead and address information; comparison sources of information; validation of information for accuracy; and documenting and updating FCMS with all of the collected data.
- Manual and batch checks against U.S. Postal Service commercially available data sets that update city and state information by zip code. These data sets do not contain PII.
- Commercial databases

FCMS itself is the source of information for the various FCMS reports the system generates (described in Question 1.1 above). These reports do not contain any PII and are solely statistical in nature.

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

The mission of DRO is to ensure the departure of all removable aliens from the United States. FCMS supports this mission by enabling DRO Officers to track and process biographical, biometric, lead, and arrest information for the purpose of locating, arresting, and removing fugitive aliens from the United States.



Fugitive alien information, to include biographical and/or biometric data, is used to facilitate the correct identification of the fugitive alien. An alien's FBI number is necessary for determining criminal history information and the A-Number is needed for determining immigration status. Additionally, any Social Security number associated with an alien is used to help confirm the correct identification of the fugitive alien.

Non-fugitive alien information is only collected in the event that a DRO Field Officer encounters an illegal alien during the process of tracking a fugitive lead and/or arresting a fugitive alien as part of enforcing the overall ICE mission. Aliens are identified as illegal non-fugitives when they are illegally present in the United States but have not been placed in immigration removal proceedings by DHS. DRO Officers verify the identity and immigration status of the non-fugitive aliens by reviewing information in Federal databases, conducting interviews, and running fingerprint checks prior to entering the encounter as an arrest of an illegal alien in FCMS. The arrest information (e.g., A-Number, arrest date and arrest location) pertaining to the alien is recorded in FCMS and serves as a statistical record of the arrest. The illegal alien is noted in FCMS as a non-fugitive alien and the information is used only for statistical reporting on the performance of the National Fugitive Operations Program. The non-fugitive alien information is not updated to reflect a change in immigration status, i.e. change from non-fugitive alien to fugitive alien or from non-fugitive alien to a U.S. citizen. Any change in the alien's immigration status is reflected in other immigration-related systems.

DHS immigration enforcement data, immigration removal case information and custody status from EID (when available), and biographical and arrest booking data from EID is used to provide any existing ICE case information that is available on the fugitive alien. Immigration case history information is used to determine the likelihood of whether the fugitive alien remains in the country or has already left the country. Criminal history information is one factor that may be used to prioritize the allocation of time and resources of the Fugitive Operations Teams to those fugitive aliens with a criminal history and assess risk.

Custody information is used to determine if any aliens with outstanding removal orders are already incarcerated. Immigration benefit data is used to help remove cases from the fugitive backlog where the alien received an immigration benefit (e.g., lawful permanent resident status) after receiving a final order for removal.

Address data from the U.S. Postal Service is used to update city, county and state information by zip code on a monthly basis. This information is used to ensure that address data tables within FCMS are routinely updated to accurately report city place names by zip code. In addition, address data and validation as indicated by batch and manual checks of commercial databases are used to increase the probability in identifying valid and credible address matches to determine where fugitive aliens could be residing.

Activity information, inputted by DRO Field Officers, is used to document and manage DRO fugitive case and arrest information. Lead information is used to assist Fugitive Operations Teams to locate fugitive aliens.



## **1.4 How is the information collected?**

Information can be collected directly from the fugitive or illegal alien at the time of arrest and/or placement into ICE custody, as well as from the DRO Officers during the arrest activities. This information is manually entered in the system. Other information is collected from internal and external systems through data extracts that are manually reviewed and edited to reduce inaccurate or corrupted data, which may include personal information, and resulting outputs are uploaded into FCMS. ICE primarily collects information from the data sources referenced in Question 1.2, which generate new fugitive alien cases and update existing case information in FCMS.

Much of the information pertaining to a particular fugitive alien that is contained within FCMS is derived from the original arrest processing of the alien in the EID system. This information is collected through a daily extract from EID. DRO Officers manually update the case data as they gather information through the arrest process and ICE custody events; the results of batch processing of addresses information from commercial sources; and the various sources of information documented in Question 1.2 to locate fugitive aliens and document arrests.

## **1.5 How will the information be checked for accuracy?**

DRO Officers manually verify and validate the lead and arrest information against information in other DHS systems when they are investigating each case in FCMS. Specifically, DRO Officers de-conflict and/or validate information contained in FCMS manually when they receive lead information and begin to investigate a fugitive alien's location. For example, when a DRO Officer receives a possible new address for a fugitive alien, he or she may run checks of EID, to verify that the individual is a fugitive before performing surveillance at the location. Any new information resulting from the manual checks and verification is entered in FCMS to provide comprehensive notes and information of the fugitive investigative process.

Internal quality control features also exist in FCMS to minimize data entry error by DRO Officers. For example, field-level validation is used to ensure appropriate data is entered into specialized fields (e.g., Social Security number fields must contain nine numerical digits, and a date field must be formatted as a date and fall within a certain date range). System defaults ensure when actions are taken, key values are automatically generated and saved. User input is limited in many cases to drop down input lists of valid responses. Before any data is saved in FCMS, if the data needs to be verified, code executes to iterate through the text boxes verifying the data. If an error exists, the user is prompted to correct it.

In addition, electronic batch audits of FCMS information occur when data extracts from other DHS systems are imported into FCMS. There are several validation and verification processes that cross check the various address and lead information obtained from external systems. These checks are a set of business rules and system logic that assist in identifying conflicting data, ranking the validity of addresses and leads, and checking for anomalies. These checks are performed regularly to ensure FCMS's data integrity by assessing the integrity and the reliability of the internal and external information stored.



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

DHS has been authorized to collect information for this program pursuant to the following authorities; 8 U.S.C. § 1103; 8 U.S.C. § 1225; 8 U.S.C. § 1226; 8 U.S.C. § 1324; 8 U.S.C. § 1360(b); 8 U.S.C. §§ 1365a and 1365b.

## 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:** FCMS could present a risk of the over-collection of PII.

**Mitigation:** ICE collects only a limited amount of information necessary to locate, arrest, and remove fugitive aliens in the most efficient manner. All PII collected is necessary to perform immigration law enforcement activities. For example, an alien's FBI number is necessary for determining criminal history information and the A-Number is needed for determining immigration status. For information collected pertaining to non-fugitive aliens, ICE only collects the minimum amount of arrest information (i.e., A-Number, and date and location of the arrest) to support statistical reporting on the performance of the Fugitive Operations Teams. The limited scope of information collected ensures that the risk of over-collection is mitigated.

**Privacy Risk:** FCMS's use of commercial data could present a risk of data inaccuracy.

**Mitigation:** ICE takes several steps to promote data accuracy and integrity when using commercial data sources. First, multiple commercial sources deemed credible and effective are used to increase the probability in identifying valid and credible address matches. Second, the commercial data providers provide results to ICE with a relevance score to help identify the most useful matches. Third, ICE assesses these results against other available information to identify workable leads, which will be investigated by DRO Officers prior to taking action affecting the individual. For example, when a DRO Officer receives a possible new address for a fugitive alien, he or she may run checks of EID to verify that the individual is a fugitive before performing surveillance at the location.

## 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.

FCMS fugitive alien information is used primarily in two ways. First, it is used to manage and document ICE investigations to locate and arrest fugitive aliens, including the generation of leads on where fugitive aliens may be currently located; the creation of Operations Plans, which describe scope of fugitive alien arrest efforts and points of contact for the Fugitive Operations Teams, local police, and emergency services personnel; and documenting Reports of Investigation, which summarize in writing the officer





activity including leads, field research and outcome (e.g., arrest). Second, FCMS information is used to generate statistical reports for management, budgeting, reporting and planning purposes within ICE. FCMS statistics are also used for reporting to Congress for program budget evaluation purposes, and for responding to requests from external parties like Congress, auditors, and the media for information about the National Fugitive Operations Program.

Information stored in FCMS about arrests of non-fugitive aliens is used only for statistical reporting purposes.

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

FCMS provides DRO Officer and alien information via screens and statistical reports. FCMS has tools that permit users to perform ad hoc queries to search for cases based on biographical information of the alien or by DRO Field Office or sub-office. FCMS also permits users to generate statistical reports as described in Question 1.1 above.

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

ICE purchases from the U.S. Postal Service a publicly available data set called City State Product. This data set contains comprehensive information about zip codes and their corresponding city and county names. This information is used to ensure that address data tables within FCMS are routinely updated to accurately report city place names by zip code. The data set is updated monthly and does not contain PII.

ICE also holds contracts with commercial public records aggregators. ICE uses more than one aggregator service to increase the probability of identifying valid and credible address matches for fugitive aliens. Commercial aggregator records call upon a wide range of address sources, thereby optimizing ICE efforts to identify a current or recent address for fugitive aliens.

ICE sends fugitive alien information to the commercial aggregators in batch extracts via email and/or initiates ad hoc searches over a secure Internet connection. The commercial aggregators receive the personal information and then electronically search their databases in an effort to find current address information. The aggregators return the addresses from the search results. ICE assesses these results against other available ICE information to determine which address information is most likely to be an accurate lead. The possible addresses obtained from commercial sources are fed into FCMS as leads for DRO Field Officers to investigate. FCMS also specifically identifies the source of the address leads for reference purposes.

## **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.**

Contracts with the commercial aggregators prohibit their sale or use of FCMS data for purposes other than providing results of commercial data queries to ICE. In addition, all FCMS users complete mandatory ICE annual privacy and security training, which stresses the importance of appropriate and



authorized use of personal data in government systems. Individuals who are found to have accessed or used the FCMS data in an unauthorized manner will be disciplined in accordance with ICE policy. Also, FCMS users are assigned access roles that are pre-designated by their position and their supervisor. Only minimum access is provided using role-based privileges to ensure system integrity. FCMS system administrators and IT support staff are trained on and required to perform their duties in accordance with ICE security and privacy procedures. These controls ensure that information is handled in accordance with the above-described uses.

## 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 described in Question 1.1 is retained in the FCMS database, as is case management information related to fugitive alien cases, such as case closure, transfer, and re-opening actions. The database also retains user transactions to add, update, and change data within the system. FCMS reports, system audit logs and back up tapes are also retained.

### 3.2 How long is information retained?

The proposed retention schedule for FCMS records is under review by the National Archives and Records Administration (NARA). Fugitive alien records are proposed to be destroyed ten (10) years after the person has been arrested and removed from the United States. The information on criminal fugitive aliens that have not been arrested and removed would be retained for 75 years from the creation of the record, in accordance with established retention schedules for immigration law enforcement records<sup>1</sup>. For humanitarian reasons, the information regarding a fugitive alien that has not been arrested and removed would be destroyed ten (10) years after the alien reaches 70 years of age, provided the alien does not have a criminal history in the United States. The information regarding a fugitive alien that has obtained legal status would be destroyed ten (10) years after obtaining legal status. A non-fugitive alien's information would be destroyed ten (10) years after arrest and/or removal from the United States, whichever is later.

Audit logs are proposed to be kept for 90 days and back up tapes for 30 days. FCMS reports would be destroyed after ten (10) years or when no longer needed for administrative, legal, audit, or other operations purposes.

---

<sup>1</sup> The current ENFORCE/IDENT SORN (DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987) reflects the 75 year retention period for immigration related criminal records. In addition, the Alien File and Central Index System SORN (DHS-USCIS-001, January 16, 2007, 72 FR 1755), which is a mixed immigration benefits and enforcement file, reflects the 75 year retention as well.



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

A proposed retention schedule has been submitted to NARA for approval.

### **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 FCMS data longer than necessary would violate the Fair Information Principle of data minimization, which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

**Mitigation:** ICE proposes to retain FCMS data for periods that are appropriately tailored to serve the purpose of the system and to maintain adequate records of the agency's activities in pursuing fugitive aliens. Non-fugitive alien information is retained for ten years, which is the minimum time it is needed to generate statistical reports on the performance of Fugitive Operation Teams. Fugitive alien information is retained for various periods that are tailored to the operational and reporting need for the data based on potential outcomes of the case, i.e., whether the alien has been arrested and removed, obtained legal status, etc. Tailoring retention periods in this manner minimizes the risk that this information is retained longer than necessary and relevant to the program and the agency's mission.

## **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?**

ICE does not share FCMS data that contains PII with other DHS components and offices. FCMS statistical reports and data may be provided to other DHS components and offices; however, these reports do not contain PII.

### **4.2 How is the information transmitted or disclosed?**

ICE does not share FCMS data that contains PII with other DHS components and offices.



#### **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.**

There are no privacy risks associated with sharing FCMS data with other DHS components and offices because only statistical data that does not contain personal information is shared.

### **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?**

ICE shares extracts of fugitive alien data with commercial data aggregators on a routine basis so that they may conduct batch and ad hoc searches of their proprietary systems to produce potential leads on the fugitive's location. ICE also shares FCMS data on an ad hoc basis with individuals and entities during the course of fugitive alien investigations to help locate the alien. Finally, ICE produces FCMS statistical reports and data that may be provided to Congress, auditors, the media, and other external recipients; however, these reports do not contain PII.

ICE does not share information pertaining to non-fugitive aliens.

#### **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 System of Records Notification (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.**

The external sharing of FCMS data described in Question 5.1 is compatible with the original collection and is permitted under the Enforcement Operational Immigration Records (ENFORCE/IDENT) SORN<sup>2</sup> (DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987), which covers FCMS data.

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

Information between ICE and the commercial aggregators is shared in batch extracts delivered through encrypted electronic transfer and in ad hoc real-time searches through a secure Internet

---

<sup>2</sup> Please visit [www.dhs.gov/privacy](http://www.dhs.gov/privacy) for additional information on the Enforcement Operations Immigrations Records (ENFORCE/IDENT) SORN.



connection. ICE shares FCMS data with individuals and organizations during the course of an investigation only when a DRO Officer deems the disclosure reasonable and appropriate for the purposes of locating and arresting fugitive aliens. The exact method of disclosure during investigations can vary, but all DRO disclosures are made in accordance with DHS policies on the safeguarding of Sensitive PII.

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

**Privacy Risk:** External disclosures could present a risk of the insecure transmission of information.

**Mitigation:** Appropriate security measures have been taken during electronic transmission of FCMS data, including encryption and use of secure Internet connections. Other means of transmission are handled securely in accordance with DHS policy.

**Privacy Risk:** This is a potential risk that commercial data aggregators will inappropriately use or disclose the FCMS data.

**Mitigation:** Contracts with the commercial aggregators prevent them from sharing or selling FCMS data to any third party, or using the data for any purpose other than providing search results to ICE.

## **Section 6.0 Notice**

*The following questions are directed at the 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?**

Notice provided by ICE to the individual prior to collection of information is limited. This PIA provides notice of the existence of the system. In addition, the ENFORCE/IDENT SORN (DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987) provides notice that information about fugitive aliens is being collected. The arrest event involving fugitives or non-fugitive aliens allows the individuals to know that law enforcement is gathering information about him/her (such as information collected at the time of booking or during interviews).

Notice to individuals is limited because providing notice to fugitive aliens would undermine ICE's efforts to locate fugitive aliens by notifying them of investigative leads that are being pursued in an effort to locate and arrest the alien. It is also limited because the collection of information generally occurs when the alien's location is unknown, therefore providing notice is impractical. Lastly, the collection of information from third parties, such as commercial aggregators, is not made on behalf or at the request of ICE. The third parties collect this information for their own purposes, and are responsible for providing appropriate notice to individuals whose information they collect under applicable laws, either on the forms used to collect the information and/or through other forms of public notice, such as Privacy Act SORNs.



## 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. Aliens that are arrested do have rights afforded to them under the U.S. Constitution to decline to provide information to law enforcement.

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

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.

## 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 the public is unaware of the existence of FCMS or that individuals may be unaware of how their personal information is being used.

**Mitigation:** Notice may be provided by the other entities that collect the individuals' information in other contexts. Furthermore, publication of this PIA provides a detailed description of the types of individuals whose information is contained in the system. In the context of a law enforcement system such as FCMS, such notice is sufficient to mitigate any risks associated with a lack of notice of the collection or uses of the information. More specific notice or the opportunity to consent to use of the information would compromise the underlying law enforcement purpose of the system and may put pending investigations and apprehension efforts 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 FCMS by following the procedures outlined in the ENFORCE/IDENT SORN (DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987). 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 FCMS 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 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](mailto: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-0655, Washington, D.C. 20528.

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

If individuals obtain access to the information in FCMS pursuant to the procedures outlined in the ENFORCE/IDENT SORN (DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987), 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 ENFORCE/IDENT 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](mailto: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-0655, 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 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 above, individuals may submit requests for information and correction as permitted by the Privacy Act, which will be reviewed and corrected on a case-by-case basis. As noted previously, the purpose of the database is to aid in locating fugitive aliens. Specifically, once these individuals are located, immigration proceedings provide an avenue to provide any redress as to such status. It is the primary responsibility of the original source data owners to maintain accurate information and provide a means for individuals to access and correct inaccurate records.

### 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 are risks of a lack of access to information and inability to seek redress and correction.

**Mitigation:** Redress is available through requests as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in FCMS could inform the fugitive alien of ICE's activities and leads in attempting to arrest him or her. Access to these records could also permit the fugitive alien to impede ICE's investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies. The existing redress procedures are adequate to address the individual's right to access and correct their records.

## 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?

Access to FCMS information is limited to only DRO employees assigned to work for or oversee the National Fugitive Operations Program, including DRO Officers assigned to the Fugitive Operations Teams. A DRO employee who seeks access to FCMS must obtain a supervisor's certification that access is appropriate and related to that individual's duties. A user request form is completed and signed by the supervisor. The roles and privileges assigned to a particular user are predetermined depending on that





user's function and position within ICE. The FCMS user roles and access are directly tied to the user interfaces within the application: Lead Access and Activity Access Menus. The available permissions allow users to have read-only, read/add/update, or full access, depending on their position and duties. There are a limited number of employees that have system administrator roles and their ability to change data is limited and audited.

## **8.2 Will Department contractors have access to the system?**

Yes. FCMS is accessed by contract support staff that provide IT development, operations and maintenance, and technical support for the system. In addition, contractors that are supporting ICE's effort to reduce the fugitive alien case backlog also have access to FCMS. No other DHS contractors have access to FCMS. Contractors are only granted access to the system when it is necessary for them to accomplish an agency function related to FCMS. All contractors must successfully complete a background investigation before they will be provided FCMS access privileges.

## **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. Additionally, system users receive training on appropriate uses of FCMS as part of DRO's Fugitive Operations Training. The FCMS User Guide also provides instructions relating to the operations and the security mechanisms built within the FCMS application.

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

FCMS completed the Certification and Accreditation process and received a three-year Authority to Operate (ATO) on June 29, 2007.

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

FCMS operates within the DHS network and is protected by DHS network firewalls. FCMS has a number of specific auditing measures and technical safeguards in place. User authentication at the network and database levels and network encryption prevent unauthorized access to FCMS data. Workstations are configured to deactivate the user's screen after inactivity and to deactivate a user id after an appropriate level of inactivity.

Audit records and user authentication (logons and logoffs) are captured by the operating system. All failed logon attempt are recorded in an audit log and periodically reviewed. The FCMS application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunctions occur. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value.



Finally, ICE has a process in place for investigating and responding to suspicious activities on the system. This process includes automated tools to assist the administrators in their monitoring, analysis, and reporting and is consistently followed.

## **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 privacy risks to this system are primarily the risks of unauthorized system access or use and inadequate system security.

**Mitigation:** These risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above, those controls include user access controls, auditing, and user training.

## **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 FCMS application is an operational system that supports the National Fugitive Operations Program as a management tool for processing, tracking, and storing information about fugitive aliens.

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

FCMS is in the operational and maintenance (O&M) phase of the System Lifecycle Management (SLM) process. The new version of FCMS is in the development phase of the SLM process and will be deployed in August 2009.



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

No. FCMS does not employ technology that raises privacy concerns.

## **Responsible Officials**

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

## **Approval Signature**

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan  
Chief Privacy Officer  
Department of Homeland Security