Privacy Impact Assessment
for the

Law Enforcement Intelligence Fusion System (IFS)

November 17, 2008

Contact Point
Susan Lane
Director, Office of Intelligence
U.S. Immigration and Customs Enforcement
(202) 514-1900

Reviewing Officials
Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
(202) 514-1900

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Intelligence Fusion System (IFS) enables ICE and other Department of Homeland Security (DHS) law enforcement and homeland security personnel to analyze volumes of information from multiple data sources through a single web-based access point. All IFS activity is predicated on ongoing and valid homeland security operations, law enforcement activities, and intelligence production requirements. IFS was formerly known as the ICE Network Law Enforcement Analysis Data System (NETLEADS). ICE has completed this Privacy Impact Assessment (PIA) to provide additional notice of the existence of IFS and publicly document the privacy protections that are in place for IFS.

Overview

Background

IFS is an ICE-operated system with two distinct purposes. First, IFS provides search and limited analysis capabilities to DHS components responsible for enforcing or administering the customs and immigration laws of the United States, as well as other laws within the DHS mission. Second, and specific to ICE, IFS acts as the repository for the ICE Office of Intelligence work product. Once finalized, this work product is also available (in varying capacities) for search and retrieval by other agencies as part of the IFS search capabilities. For clarity, this PIA will discuss these two functions separately.

IFS Search Capabilities

On a basic level, IFS is a software application that uses tools to search and analyze large volumes of data to support DHS law enforcement intelligence and investigative activities and the administration of U.S. immigration laws. IFS (NETLEADS) was created in 1997 by the Immigration and Naturalization Service (INS), a U.S. Department of Justice component whose functions and personnel were transferred to DHS in 2003. INS created IFS to centralize immigration and related law enforcement data to allow more efficient search and analysis by INS's immigration and law enforcement personnel. Over time, INS added additional data sets and tools to enhance users' ability to conduct searches and identify associations or links between individuals that may be relevant to immigration or law enforcement activities.

During DHS's creation, the system was transferred to ICE and the original system users, who now worked for ICE, U.S. Citizenship and Immigration Services (USCIS), and U.S. Customs and Border Protection (CBP), kept their access. Since IFS transferred to DHS, additional users have been added from these agencies and other parts of DHS and IFS's purpose has been expanded beyond immigration to also support DHS law enforcement intelligence and investigative activities generally.

IFS allows authorized DHS immigration officials, law enforcement personnel, and intelligence analysts to increase the efficiency of multiple data source searches and identification of similar, identical, or related information from disparate datasets. Users can quickly search large amounts of structured and

unstructured data to identify individuals, groups, incidents, or activities based on user-defined parameters or queries.

DHS personnel also use IFS to conduct research for intelligence reports in support of the administration of immigration laws and other laws administered or enforced by DHS, law enforcement activities and investigations, and law enforcement intelligence analysis. IFS uses role-based access controls to limit user access to only those databases that are appropriate for their job and agency responsibilities.

IFS is specifically designed to make the process of researching and analyzing separate data sets more efficient for its users. IFS relieves users of the need to individually and manually access key DHS immigration and law enforcement databases to conduct research or obtain records about a particular individual or organization of interest. IFS users save valuable time by no longer maintaining multiple user names and passwords for each data source and logging into each data source separately.

IFS also reduces the privacy risks that exist when users conduct research in multiple unconnected systems. Separate systems return results in separate interfaces, making the task of consolidating, comparing, and analyzing those results time consuming and difficult, and increasing the likelihood of human error. Further, separate system queries increase the likelihood that users may overlook important investigative and intelligence connections that might only be revealed if they were able to access multiple data sources simultaneously.

IFS provides a simple link visualizing tool which allows a user to see a visual representation of the links between documents he retrieved. For example, if a user retrieves records in IFS on "John Doe," all the records related to John Doe will be retrieved and tagged as having come from a specific source system. The user will click on the link visualizer which will create a visual representation of the links between those documents. The visualizer does not perform any analysis other than linking the documents retrieved by the user query; the visualizer is simply another way to view text search results.

IFS and the ICE Office of Intelligence

The ICE Office of Intelligence (ICE Intel) uses IFS to generate reports and conduct initial research into subjects of interest, and as the primary repository for finished law enforcement intelligence products. In addition, ICE Intel uses IFS to manage its workflow related to the drafting of law enforcement intelligence products.

For example, an ICE analyst will research an issue that is of interest to ICE field agents. Once the analyst and his superiors are satisfied the research warrants an ICE-generated intelligence report, the analyst will draft a report using a report template provided by the ICE Intel portion of IFS. The draft report will be distributed through IFS for review and clearance to supervisors in ICE Intel. Once finalized and approved, the final report will stored in IFS and also be available through IFS to those component or agency employees who have privileges to view such reports from ICE Intel.

Two specific examples of such reporting are the Homeland Intelligence Reports (HIRs) and Homeland Security Intelligence Reports (HSIRs). HIRs contain raw, unanalyzed information about suspicious or illegal activity reported by ICE law enforcement officers and agents. HSIRs are reports of suspicious or illegal activity that also contain the results of research and analysis by ICE Office of

Intelligence analysts and agents. Both HIRs and HSIRs are dated and include information about the suspicious or illegal activity, relevant program area (e.g., gangs, alien smuggling), identifying information about the individuals involved (subjects, associates, or others), and the information source. HSIRs also contain the results of research and analysis, such as key findings of the information, background information and additional information on the subjects. This report also contains suggested follow-up actions and the names of associates.

Information Sources

IFS uses immigration, border, visa, law enforcement, intelligence, and incident information collected by DHS and other Federal, State and local agencies, as well as open source data. This information includes personally identifiable information (PII). IFS information is either structured or unstructured. This information is available for search within IFS based on the privileges and roles granted to IFS users based on ICE and their home agency's mission requirements.

Structured Data

Structured data is made up of the reports and files contained in several databases across DHS and other Federal and state agencies. These reports are searchable by specific data elements: name, date of birth, alien registration number, Social Security Number, etc. Searches may retrieve several documents from several databases (assuming the user who made the query has privileges to view those databases containing responsive results) and list them for the user, noting specifically the original source system from which the document was retrieved.

The user may use a link analysis tool which will visualize the connections between the retrieved documents; this link analysis, however, is premised only on the facts of the structured text. This means that similar names will be linked, similar addresses will be linked, and so on. The analysis is not sophisticated or predictive; the link analysis requires the analyst to further research and support any findings relevant to his final report or product. IFS makes no decisions about the significance of any relationships; it only identifies possible connections for DHS personnel to verify through independent research or investigation and then evaluate the importance of those connections using judgment and experience. Structured datasets are reviewed for appropriateness before being made available in the link analysis tool.

Unstructured Data

No link analysis is available under unstructured text searches because the text is unstructured; this means that IFS does not define any data elements (such as name or address) prior to search retrieval, making the text "unstructured" and not linkable without specific research by the analyst. To search the unstructured data in IFS, users enter search terms that the system will use to retrieve records containing those terms. Users can also use Boolean searches to narrow their search and increase the likelihood of finding relevant records. Searches of structured and unstructured data cannot be performed simultaneously in the system.

In order to assess the privacy issues associated with the collection, maintenance, and use of the PII that is maintained in IFS, which includes necessary sharing with other agencies, the DHS Privacy Officer directed that a PIA be performed in accordance with Section 208 of the E-Government Act of

2002, and that the PIA be periodically updated as necessary to reflect future changes to IFS. Notice of the existence and operation of IFS is provided by this PIA, and the ICE Intelligence Records System (IIRS) SORN and Notice of Proposed Rulemaking (NPRM) published in the *Federal Register*.

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?

IFS contains and/or retrieves a broad range of information from various sources within ICE, DHS, other Federal agencies, State and local agencies, and news media outlets. This information may be structured (information culled from structured databases), and unstructured (media reports and various unformatted reports, for example). The specific categories of information are as follows:

1. Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies
2. U.S. visa, border immigration and naturalization benefit data, including arrival and departure data
3. DHS immigration and law enforcement data
4. Terrorist watchlist data
5. Data on individuals not authorized to work in the United States
6. Lost and stolen passport data
7. Open source and press reports

The specific PII elements vary by category, but generally may include some or all the following: name, photograph, aliases, date of birth, citizenship and immigration status, nationality, immigration benefits, immigration history, admission information, customs import-export history, criminal arrest and conviction record, alien registration number (A-Number), phone numbers, addresses, identification document numbers, criminal associations, family relationships, employment, military service, education and other background information.

For structured content datasets, the data fields included in the index are typically name, date of birth, alien number, passport number, country of birth/citizenship, and other key identifiers.

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

The systems contain law enforcement, visa and immigration, border inspection, suspicious incident reporting, criminal history, and commercial or public information.

Generally, Enforcement Operational Immigration Records (ENFORCE) (DHS/ICE-CBP-CIS-001-03, Enforce/IDENT Mar. 20, 2006, 71 FR 13987) and Treasury Enforcement Communications System (TECS) (Oct. 18, 2001, 66 FR 52984) information is collected directly from individuals during an encounter with DHS. Other data are obtained directly from persons applying for U.S. immigration benefits or admission to the U.S. This information is collected by the DHS Student and Exchange Visitor Information System (SEVIS) (DHS/ICE-001, Mar. 22, 2005, 70 FR 14477), and the U.S. Citizenship and Immigration Services (USCIS) immigration benefits applications and application review systems, including CLAIMS 3 and CLAIMS 4 (DHS-USCIS-007, Sept. 29, 2008, 73 FR 56596). Some information is also taken from ICE's General Counsel Electronic Management System (GEMS) (DHS/ICE/OPLA-001, Mar. 31, 2006, 71 FR 16326), LEADTRAC, and ICE iDOX. Other information is obtained from the Transportation Security Intelligence Service (TSIS) Files (DHS/TSA 011, Dec. 10, 2004, 69 FR 71828) about individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

These sources contain structured data (e.g., Oracle, Microsoft and mainframe database content), unstructured data (e.g., textual reports, open source documentation, web pages, Reports of Investigation narratives, PDF files), or both. IFS does not directly collect information from individuals.

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

IFS centralizes information collected by the sources of information listed in Questions 1.1 and 1.2 above to support law enforcement activities and investigations of violations of U.S. laws, administration of immigration laws and other laws administered or enforced by DHS, and production of DHS law enforcement intelligence products. Specifically, IFS automates the following business processes:

- Analysis of leads, law enforcement and intelligence reports, and referrals, and processing of queries of DHS and other Federal agency information to locate relevant records and produce reports.
- Integration and resolution of information from multiple DHS and Federal agency databases to provide leads for law enforcement investigations and disruption of potential terrorist activities.
- Initiation of analyses that support law enforcement activities and investigations and the administration of immigration benefits.
- Production and dissemination of law enforcement intelligence reports.
- Management of analysis workflows and information resources.

As stated in the Introduction, IFS allows authorized DHS agents, investigators, officers and analysts to increase efficiency of multiple data source searches and identification of similar, identical, or related information from disparate datasets. Users can quickly search large amounts of structured and unstructured data to identify trends or connections among multiple individuals, groups, incidents, or activities based on user-defined parameters or queries. DHS personnel also use IFS to generate intelligence reports for purposes of administration of immigration laws and other laws administered or enforced by DHS, law enforcement activities and investigations, and law enforcement intelligence analysis.

1.4 How is the information collected?

With the exception of the ICE-generated intelligence reports discussed below, IFS is not the initial collector or generator of any information it receives. Information collected in other databases is received by IFS through various means, including CD-ROMs, electronic messaging, and direct electronic connection. The information is indexed for searching and loaded into the IFS data repository. For some data sources, IFS electronically retrieves records directly from the data source in response to a user request to view a particular report or record. For other data sources information is stored directly in IFS's data repository.

For ICE-generated intelligence reports, IFS is the original system of records, and the reports are based on information received by ICE from various sources (see Question 1.2).

1.5 How will the information be checked for accuracy?

Other than as described in Question 3.2, IFS is not the original system of record for most its the source data. Source data is collected by other systems and IFS relies on those systems and system owners to have appropriate processes in place to ensure their data is accurate. Because of the law enforcement and intelligence context in which IFS is used, it is usually impossible to directly verify the accuracy of information with the individual about whom the specific information pertains. However, because IFS is used by multiple DHS components and offices, users other than the data owner who hold relevant knowledge have the opportunity to correct inaccuracies when they are discovered. Users that have access may directly query source databases or other government databases to verify the accuracy of IFS information; when source systems are updated IFS will also be updated based on the manner in which IFS receives information from the source system (electronically or physical copy). If necessary and when available, users may also consult a commercial data provider to verify information but that verification does not occur within IFS.

With respect to the production of ICE-generated intelligence reports, ICE Intel personnel receive training on the importance of verifying information prior to including it in those analytical reports and it is standard practice to remove or correct ICE-generated intelligence reports from the IFS data repository if they contain inaccurate information that may prejudice an individual.

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

ICE has been authorized to collect information under 5 U.S.C. §301; 8 U.S.C. §1103 and 1105; 8 U.S.C. §1225(d)(3); 8 U.S.C. §1324(b)(3); 8 U.S.C. §1357(a); 8 U.S.C. §1360(b); 19 U.S.C. § 1; and 19 U.S.C. § 1509.

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

The primary risk associated with collecting this data is that users will not be aware that this information is being aggregated in this manner and for law enforcement intelligence purposes. In order to increase transparency, ICE has published a SORN and this PIA as the means of informing individuals about the specific elements of IFS.

Additionally, there is a privacy risk associated with allowing an information system to make decisions about the relevance or value of data. This is mitigated by the fact that DHS agents/analysts are: a) legally authorized to perform the activity (i.e., law enforcement intelligence gathering, analysis, and reporting), b) submitting specific search parameters based on law enforcement investigations/activities and suspicious activities identified by agents/analysts based on their judgment and experience, and c) reviewing any and all results displayed by IFS to determine if further action is warranted. Human review of the relevance and quality of data provides a measure of protection against unreasonable links and associations made by a computer's analysis. These measures ensure that agent/analysts are responsible for any ultimate decisions, not IFS. Finally, agents/analysts are trained in the correct use of privacy information to ensure that the privacy of individuals is protected.

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.

IFS searchable information, including ICE-generated intelligence reports, is used to support law enforcement activities and investigations of violations of U.S. laws, administration of immigration laws and other laws administered or enforced by DHS, and production of DHS law enforcement intelligence products. IFS indexes the all-source information for search and analysis. Indexing results in the capture of different amounts and types of data depending on whether the data source contains unstructured (i.e., free-text) data or structured data

ICE-generated intelligence reports are used to document and conduct activities related to ongoing law enforcement intelligence research and investigations.

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

Tools and Analysis of IFS Searchable Data

IFS provides an integrated common interface for the search and analysis of intelligence, law enforcement, border, visa, and immigration information. IFS provides information technology tools to assist IFS users in recognizing relationships among persons, resolving addresses collected in varied formats, understanding organizational relationships using information within existing databases, and developing timely, actionable leads needed to accomplish law enforcement and law enforcement intelligence objectives, and administration of immigration laws and other laws administered or enforced by DHS.

IFS's analytical tools increase the efficiency of data search and analysis conducted by DHS personnel. IFS's "matrix search" tool allows users to search unstructured data using more combinations of Boolean searches than a traditional Boolean search tool would allow. The matrix tool results will provide the user with more potential combinations of record results to choose from than a traditional Boolean search. IFS also has the capability to query narrative text to efficiently locate established or ad hoc word strings or context statements. This enables the comparison of vast quantities of information in electronic format to identify potentially fraudulent claims for immigration benefits

Another IFS tool allows users to search multiple structured-content datasets using a single query, sometimes referred to as a federated search. This is one of the critical values of IFS. Such searches prevent analysts from searching multiple databases independently, saving hours of work which would otherwise be taken up logging into several different systems.

In response to user-specified queries IFS can also conduct link identification which identifies links between individuals based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information they may help agents and analysts identify potentially criminal or suspicious activities and the individuals associated with them.

These various tools allow IFS users to produce analytical results on their screens using the capabilities described above. These results are a different way of looking at the original data. IFS users can save search results or source documents identified during a search to their local workstations in electronic format, but IFS does not create new documents as the result of user searches and does not save any data regarding the links identified.

Tools and Analysis of ICE-Generated Intelligence Reports

Aside from the analytical tools described above, IFS also contains tools available only to ICE Office of Intelligence users that assist agents and analysts with the generation, version control, and approval of ICE-generated intelligence reports. IFS is the official repository for ICE-generated intelligence reports.

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

IFS search data and ICE-generated intelligence reports use publicly available news media information, e.g., reporting from the Associated Press (AP). Analysts and agents can use the information from the AP to enhance their intelligence reports. For example, a search of AP press reports could alert ICE to an alien's recent conviction for a violent crime which renders the alien deportable under U.S. immigration law. IFS also uses publicly available maps and satellite data from Google. Analysts use these maps to visualize subject addresses and determine proximities to one another, which may be used for law enforcement and law enforcement intelligence objectives, and administration of immigration laws and other laws administered or enforced by DHS.

Analysts may also use commercially available data to verify information they have retrieved from IFS; however commercial data is not a source system for IFS searches. Agents and analysts have separate access to commercial data as part of their operational duties, regardless of the existence and operation of IFS.

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.

As described in Section 8, security and access controls and audit processes are in place to mitigate the risk that personally identifiable information will be accessed by unauthorized individuals or for unauthorized purposes. IFS users receive computer security and privacy awareness training to mitigate the risk that information will be used inappropriately.

There are several risks associated with the use of a link analysis tool, albeit a simple tool like the one used in IFS. First, there is a risk exists that IFS is making important decisions about investigations or individuals, rather than human agents/analysts who are able to exercise experience, discretion and judgment. This is not true of IFS. IFS is not the sole basis for any decisions made by DHS personnel about individuals. IFS makes no decisions about the significance of any relationships; it only identifies possible connections for DHS personnel to verify through independent research or investigation who then evaluate the importance of those connections using judgment and experience. DHS personnel that use IFS to generate analytical reports are trained to verify information before including it in the report, thereby minimizing the risk that inaccurate data will be perpetuated.

Second, the link analysis tool could present information based on inaccurate information, thereby corrupting the links provided to the user. Similar to the risk above, this is mitigated by requiring analysts and users to verify their information before acting upon it; i.e., including it in a report or product.

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?

ICE retains the records in the IFS data repository, including the ICE-generated intelligence reports. IFS stores in the IFS data repository the full content of unstructured datasets and indexes of certain fields of structured datasets.

3.2 How long is information retained?

Records for Which IFS is not the System of Record (source data)

IFS datasets that are copies imported from other DHS or Federal systems will be retained in IFS for twenty (20) years to support research and analysis by IFS users. The inputs to IFS (emailed zip files, CD-ROMs, etc.) will be destroyed after upload and verification to IFS, or returned to the source.

Records for Which IFS is the System of Record (ICE Office of Intelligence Records)

ICE is in the process of drafting a proposed record retention schedule for the information maintained in IFS. ICE anticipates retaining the IFS datasets for which IFS is the repository of record for 75 years. This retention period is 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. Those datasets are:

- Student and Schools System (STSC) – Records from legacy INS containing basic information on INS-certified schools and the foreign students who entered the United States with I-20s (form used for processing student visas) issued by these schools. This is a closed dataset that is no longer updated or active. Since 2004, this type of information has been maintained in the ICE Student and Exchange Visitor Information System (SEVIS), which has a retention period of 75 years.
- Criminal Investigative Reporting System (CIRS) – Records from legacy INS criminal investigative files. This is a closed dataset that is no longer updated or active.
- ICE-Generated Intelligence Reports – Law enforcement intelligence reports produced by the ICE Office of Intelligence in IFS and maintained in the IFS data repository. This is an active dataset that is continuously updated.

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

No. ICE is in the process of drafting a proposed record retention schedule for the information maintained in IFS.

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

IFS datasets that are copies imported from other Federal systems are retained for 20 years, which is an appropriate period to support the law enforcement and immigration purposes of IFS. A shorter retention period would significantly decrease the value of IFS as a research and analysis tool and impair the very efficiencies it was intended to create. IFS datasets for which IFS is the repository of record are maintained for a longer period of time (75 years) because those are the official record copies of that information. This retention period is appropriate because it is consistent with the retention periods generally established for criminal investigation records, immigration records, and law enforcement intelligence products. These records are relevant and may be necessary to the DHS mission over the lifetime of the individuals involved.

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?

For IFS search capabilities, ICE grants IFS user accounts to other DHS personnel for the purpose of facilitating law enforcement and law enforcement intelligence objectives, and administration of immigration laws and other laws administered or enforced by DHS. Specifically, select personnel from CBP, USCIS, TSA, U.S. Coast Guard and DHS Intelligence & Analysis have IFS user accounts which allow them to log into IFS, access the data in the IFS repository and use the IFS analytical tools.

ICE Intel may share ICE-generated intelligence reports stored in IFS with other DHS components to facilitate law enforcement and law enforcement intelligence objectives, and the administration of immigration laws and other laws administered or enforced by DHS. The information will be shared to the extent that the DHS component has demonstrated a need to know and the use for the information falls within that component's statutory mission.

4.2 How is the information transmitted or disclosed?

IFS users within DHS access IFS electronically through the secure DHS network. ICE-generated intelligence reports are transmitted via hand-delivery or first-class mail, or via email or file transfer over secure DHS sensitive but unclassified (SBU) networks. Reports are marked "For Official Use Only/Law Enforcement Sensitive." As a pre-condition to receiving such reports, ICE prohibits the recipient agency from further disseminating the information without prior approval from ICE.

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.

IFS includes the following safeguards to mitigate internal information sharing and privacy risks: controlling system access, providing security and privacy training for IFS users, and allowing the transmission of data only through the secure DHS network. In addition, users take annual security and privacy training and also acknowledge user behavior rules through the IFS system every 90 days. These measures ensure that any internal sharing of data is done within the technical and policy guidelines of DHS and its components.

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?

For IFS search capabilities, ICE does not permit any external (i.e., non-DHS) agencies or organizations to have privileges to access IFS.

ICE Intel shares ICE-generated intelligence reports with law enforcement or intelligence agencies that demonstrate a need to know the information in the performance of their missions, including Federal, State, tribal, local and foreign law enforcement agencies, as well as relevant international organizations such as INTERPOL. The U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) receive analytical reports, but external sharing is not limited to those agencies. Reports are shared with any U.S. law enforcement or intelligence agency that demonstrates a need to know to further its own law enforcement analyses or investigations. All sharing is in accord with the IFS SORN and the Privacy Act of 1974.

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

preparation for, in aid of, or related to terrorism. This sharing is in accord with the routine uses published in the IFS SORN.

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.

The IFS SORN applies to IFS information and includes routine uses to permit external sharing for law enforcement, homeland and national security, audit, congressional, data breach, litigation, and records management purposes. This external sharing is compatible with the immigration and law enforcement mission of ICE, and the purposes of IFS. The ICE-generated intelligence reports are products of law enforcement intelligence research and analysis and are distributed on a case-by-case basis to authorized law enforcement and intelligence agencies consistent with the reason for collection of the source information and the routine uses that are to be published in the IFS SORN concurrently with this PIA.

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

ICE-generated intelligence reports are transmitted via hand-delivery or first-class mail, or via email or file transfer over U.S. Government sensitive but unclassified (SBU) networks. IFS analytical results are considered law enforcement sensitive data, and this data is typically shared with other law enforcement agencies which have proper procedures and training in place to safeguard such investigatory data. Reports are marked as "For Official Use Only/Law Enforcement Sensitive." Prior to any information being shared, the recipients would be required by ICE to safeguard the information in accordance with its sensitivity, and prohibited from further disseminating the information without prior approval from ICE.

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

The external sharing of information described above is consistent with Federal homeland security information sharing mandates codified by statute, executive order, and agreement. ICE has appropriate measures in place to secure the information during transit and to validate the information's accuracy before ICE takes any action that is adverse to an individual. ICE shares ICE-generated intelligence reports only with law enforcement and intelligence organizations that have demonstrated a need to know the information in the course of their official duties. DHS-mandated security and privacy training also mitigate the risk that IFS users will share or handle sensitive information improperly.

ICE-generated intelligence reports are distributed on a case-by-case basis to authorized Federal law enforcement and intelligence agencies consistent with the reason for collection of the source information and the routine uses in the IFS SORN.

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?

IFS does not directly collect information from individuals. IFS analyzes information collected in other databases, some of which is collected directly from individuals. This PIA and the IFS SORN (published concurrently with this PIA) serve as public notice of the existence, contents, and uses of the IFS system. With respect to information obtained from individuals through government forms or other means, such as immigration benefits applications, notices on the forms state that their information may be shared with law enforcement entities. As part of this PIA process, DHS reviewed the applicable SORNs to ensure that the uses were appropriate given the notice provided.

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

In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, opportunities to decline may be limited or nonexistent. Specific to IFS, because IFS is not the direct collector of any of its information, IFS is not in the best position to provide an opportunity to decline to provide information.

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

In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, no such consent exists. Specific to IFS, because IFS is not the direct collector of any of its information, IFS is not in the best position to provide an opportunity to consent to provide information or the use of that 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.

The risk that individuals may not be aware that their information may be contained within IFS is mitigated primarily by the public notice provided through this PIA and the IFS SORN. In addition,

individuals are notified at the point of collection of the original data that their information may be shared for law enforcement purposes. Additional notice is not provided to individuals because IFS is a fusion system that places intelligence reports, incident reports, and copies of other government datasets into a single repository so that search and analysis can be performed more efficiently for authorized law enforcement and intelligence purposes. Because IFS is a system used for law enforcement purposes, additional 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 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 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 component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

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 component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The procedure for submitting a request to correct information is outlined in the ICE Intelligence Records System 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.

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 IFS and the data that 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. In addition, because IFS contains copies of datasets owned by DHS components and offices or other agencies, individuals may also have the option to seek access to and correction of their data directly from those agencies or offices that originally collected it. Information that is corrected in the original data source will be updated in the IFS data repository during routine refreshes thereby ensuring accurate and current 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. The IFS administrator can elect to assign all the privileges for a given role or can select only certain privileges to assign. IFS access is limited to those personnel who have a need to access the system based on their roles in support of law enforcement and law enforcement intelligence activities, or the administration of immigration laws and other laws administered or enforced by DHS. The IFS roles are:

- ICE Office of Intelligence User Roles: All ICE Office of Intelligence users can search the IFS data repository, use the analytical tools in IFS, and save search strings for unstructured data searches to the system for use by other IFS users. These users also have different privileges to create, edit, view, and/or approve intelligence reporting products depending on their specific job category.
- Read-Only Users: General users within DHS, including non-Office of Intelligence ICE personnel, who have read-only privileges. This permits access to and search of the data repository and use of the analytical tools in IFS. Read-only users may save search strings

for unstructured data searches to the system for use by other IFS users. These users cannot upload content to or create reports in IFS.

- Administrative Users: Users who have read-only privileges to IFS, except they are also permitted to manually upload updates to existing data source content.
- IT Support Users: System administrators, technical and security personnel, and help desk personnel who have privileges to perform functions such as account management, password resets, and assigning and managing roles.

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 that users have the appropriate access. Individuals who no longer require access are removed from the access list. The IFS administrator (within the ICE Office of Intelligence) 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. Contractors working for DHS components and offices that have access to the system may also have access to IFS. For example, the ICE Office of Intelligence employs contract analysts who are given user privileges to IFS to perform the research, analysis, and reporting described in this PIA. Certain IT contractors have access as necessary to complete information technology development and operations and maintenance tasks on the system. All contractors undergo an extensive background investigation prior to accessing IFS or other DHS systems.

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

There is no system-specific training requirement for IFS users at this time. All ICE employees are required to complete annual privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. Additionally, all DHS personnel are required to complete some form of annual computer security training. Every employee that accesses IFS must initially and every 90 days thereafter digitally sign a "Rules of Behavior" agreement, which includes provisions to protect sensitive information from disclosure to unauthorized individuals or groups.

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

Yes. The IFS Certification and Accreditation was awarded on July 31, 2008.

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

IFS uses database-level auditing to capture information associated with any viewing, inserting, updating, or deletion of records in the dataset, and the user that performed the activity. The IFS audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. 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 IFS Information System Security Officer will review audit trails at least once per week, or in accordance with the System Security Plan. The IFS 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. The same module that manages roles and permissions is designed to automatically detect unauthorized activities.

ICE also 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. The process is consistently followed. Additionally, IFS runs within the DHS network and is protected by DHS network firewalls.

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?

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

Section 9.0 Technology

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

9.1 What type of project is the program or system?

This project is currently operational. It is an application database with data analysis tools supporting law enforcement and law enforcement intelligence objectives, and administration of immigration laws and other laws administered or enforced by DHS.

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

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

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

A privacy risk is presented by the tools used in IFS that make decisions about the relevance or value of data being searched. This is mitigated by human review of the relevance and quality of data provides a measure of protection against unreasonable links made by a computer's analysis. This process ensures that human agent/analysts are responsible for any ultimate governmental decisions, not IFS.

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security