



Privacy Impact Assessment
for the

IDOCX System

October 14, 2009

Contact Point

James Woosley

Acting Director, Office of Intelligence

U.S. Immigration and Customs Enforcement

(202) 732-5248

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

IDOCX is an information system owned by U.S. Immigration and Customs Enforcement (ICE). The system supports the collection, organization, and analysis of paper and electronic documents for law enforcement and other programmatic or administrative purposes. ICE conducted this Privacy Impact Assessment (PIA) because IDOCX collects, analyzes, and stores personally identifiable information (PII).

Overview

IDOCX is owned by the ICE Office of Intelligence (INTEL) and is designed to collect and analyze paper and electronic documents collected during the course of a criminal investigation and other law enforcement activities. IDOCX contains tools that support (1) the scanning of paper documents into electronic form and the importation of electronic documents; (2) the cataloging, analysis and extraction of data from those documents; (3) the creation of an indexed database of related documents for an investigation or project; (4) and the translation of records in a foreign language into English. In addition to its law enforcement use, IDOCX may also be used for non-law enforcement purposes within ICE in support of administrative or programmatic projects that seek to “digitize” large amounts of paper records (e.g., digitization of employee training certificates). On occasion, ICE also uses IDOCX to support digitization projects at the request of other DHS components and offices.

Not all investigations, activities, and projects use IDOCX; it is up to the individual ICE case agent or project manager to decide whether to use IDOCX. The actual information collected in IDOCX will depend on the nature of the particular investigation or project that the system is being used to support. IDOCX does not serve as a case management system for ICE investigations or as an official repository for any specific type of agency records or evidence. It is solely a support system used to assist in the electronic collection and analysis of documents.

Background

ICE performs criminal investigations and other law enforcement activities in support of its mission to protect national security by enforcing U.S. customs and immigration laws. During the course of these investigations and activities, ICE may collect paper and/or electronic documents through means such as the execution of search warrants and subpoenas, or voluntary production by individuals and entities. ICE collects a variety of documents such as business records, passports and other identity documents, documents containing biometric information (photographs and fingerprints), employment documents, criminal records, handwritten materials, and receipts.¹ In the past, ICE personnel would be required to manually review and translate documents to gather relevant information, which required significant investments of time and resources. To better support the collection, cataloguing, and analysis of these documents in an efficient and cost-effective manner, ICE developed the IDOCX system. IDOCX

¹ IDOCX is not a biometric information collection system. It does not electronically collect fingerprints from individuals or take and store photographs. Any biometric information that IDOCX processes is already present in the paper or electronic documents being collected by ICE, and is not taken directly from individuals.



automates the processes associated with document and data collection, analysis, and translation that would otherwise be performed manually by ICE personnel.

IDOCX also helps to organize documents for each project or investigation. IDOCX's organizational capabilities are versatile and can support the preferred organizational structure of various investigations and projects. For example, during the course of an ICE investigation, agents conduct a search of a business and collect documents from various locations in the office (e.g., central file room, individual offices, etc.). If the location of the documents is the preferred means to organize the records, the ICE agents will request that IDOCX organize the electronic documents by the location in which they were found. ICE personnel will scan the documents into the system in batches based on the location, and IDOCX will electronically tag the records accordingly. Later, agents can electronically retrieve all the documents found in a particular location in the office using the XML tags assigned by IDOCX.

Step One: Document Collection

The IDOCX process begins with the collection of the documents themselves which occurs by importing the paper and/or electronic documents into the IDOCX database server. If electronic document import occurs, an IDOCX system administrator will manually import files provided by ICE case agents. At no point in time do IDOCX system administrators search the contents of confiscated media; all such searches for relevant or responsive materials are performed by ICE agents only. IDOCX supports scanning at ICE Headquarters offices, or at other field locations. Field-based scanning usually occurs at an ICE field office or at other sites during a law enforcement operation such as a worksite enforcement operation or the execution of a search warrant or subpoena. ICE agents or IDOCX personnel travel to a collection site carrying mobile scanning kits that include: scanning stations (laptops and scanners), a portable server, and a network switch. Once the system has been assembled, scanning can begin. Paper documents are scanned at the scanning stations, and sent through the network switch to be stored on the portable database server. When all the documents have been scanned, the mobile scanning kit is returned to ICE Headquarters for the next step of processing. Scanning at ICE Headquarters occurs in an IDOCX Lab that contains the same equipment as a mobile scanning kit.

IDOCX can import electronic documents of various formats including but not limited to: Tagged Image File Formats (TIFF Images), Portable Document Format files (PDF Files), JPEG Images, Microsoft PowerPoint Documents (PPT Files) and Microsoft Word Documents (DOC Files). Unsupported document formats may require manual conversion to a supported format or may be printed and imported via the scanning process. Electronic documents are typically loaded onto the IDOCX database server using compact discs (CDs) or external storage devices.

Step Two: Document Analysis

Once documents have been stored in the IDOCX database server, the following IDOCX analytical tools may be used to analyze the content of the documents:

- Optical Character Recognition (OCR) Tool. The IDOCX OCR tool is used to translate images of documents (i.e., TIFF, PDF, or JPEG files) that contain typewritten or hand-printed² text into

² The OCR tool maybe able to convert hand-printed block-letter handwriting into machine-readable data, but it will be of lower accuracy than typewritten text. Most other handwriting will not be computer readable.



machine-readable data. When a paper document is scanned into a computer, the computer creates an image file of the document that is similar to a photograph. While the human eye can read the scanned document file to identify specific words, a computer cannot. By recognizing the fixed shape of different characters, the OCR Tool “translates” the numbers and letters in these image files into computer-readable and searchable text files. The text file is then associated with the scanned document file in the IDOCX database server, and it can be searched electronically for specific words or information.

- Machine Translation Tool. If IDOCX collects documents that are in a foreign language, the Machine Translation Tool can automatically translate the document into English. This tool can perform machine translations in 157 languages.
- Human Translation (HT) Support Tool. This tool supports the human translation of a document from a foreign language into English. In the event a human translator is engaged to translate a document, a separate Human Translation file will be used to retain the translation. The HT file can also be used to retain a translation of handwritten documents that the OCR tool is unable to process.
- Extensible Markup Language (XML) Tool. Following the OCR and Extracted Text processes, IDOCX creates an XML file. XML files are unique in that they aid information systems in sharing structured data. In this case, the XML file acts as the bridge that connects IDOCX’s data with Intelligence Fusion System’s (IFS) functionality. If a user wants to add information to a scanned document, such as what time and date it was scanned, this information is placed within the XML file.

Depending on the purpose of a particular investigation or project, the case agent or project manager will determine where the records are sent once IDOCX processing is complete. In some instances, the electronic records from IDOCX are sent to the case agent or project manager. In other instances, the records are exported to the ICE Intelligence Fusion System (IFS), a large data repository that provides search and analysis capabilities to DHS personnel responsible for enforcing or administering the customs, immigration, and other laws within the DHS mission. Access to IDOCX records within IFS is typically limited to only certain users based on a need-to-know in the context of particular projects or investigations.

Typical Transaction

In a typical transaction, ICE agents conduct an investigation in which they collect both paper and electronic documents. The agents determine that the documents are pertinent to the investigation and require further analysis. The agents will either request the IDOCX team to conduct on-site scanning at the collection site, or they will deliver the documents to the IDOCX team for scanning at ICE Headquarters. The agents will also provide the IDOCX team with the electronic documents to load into IDOCX, the type of analysis that needs to be performed (e.g., OCR, machine translation), the preferred organizational structure of the records if any, and whether the records should be exported to IFS when completed. The IDOCX team will then process each document through IDOCX. IDOCX creates and stores multiple associated files for each document processed. If the agents so requests, the completed records are copied from IDOCX into IFS where the agents can access the records. Otherwise, a copy of



the IDOCX records is sent to the agent or project manager on CD. The CD is encrypted with a password and sent by trusted courier (FedEx, UPS, USPS) to the agent. The agent is provided the password directly.

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?

IDOCX may collect information related to ongoing law enforcement investigations, other law enforcement activities (e.g., I-9 audits), and other non-law enforcement projects and programs conducted by ICE or other components and offices within DHS. An example of use of IDOCX for non-law enforcement purposes is the digitization of a particular set of agency records (e.g., internal training records) from paper to electronic form to enhance the efficiency of agency recordkeeping. Not all investigations, activities, and projects use IDOCX; it is up to the individual case agent or project manager to decide whether to use IDOCX. The actual information collected will depend on the nature of the particular investigation or project that the system is being used to support.

IDOCX may be used to support law enforcement investigations and activities in areas within the scope of ICE or DHS enforcement authorities, e.g., national security, customs violations, immigration benefits fraud, human smuggling, human rights violations, and gang investigations. The types of individuals on whom information could be collected in these contexts varies on a case-by-case basis, but may include subjects of investigations, witnesses, victims, business associates, customers, friends, relatives, or others whose information is among the records seized or otherwise collected during the course of the investigation. Listed below are general types of records that IDOCX could collect in a law enforcement context:

- **Identification Documents:** passports, identification cards, drivers licenses, and documents with biometric information including but not limited to photographs and fingerprint cards
- **Employer Documents:** work schedules, billing documents, waybills, I-9 forms
- **Employee Documents:** employment authorization cards; payment receipts
- **Legal Documents:** criminal records; court documents
- **Miscellaneous:** letters and receipts

The specific PII collected in these records will vary based on the nature of the records themselves. PII collected may include name, social security number, photograph, aliases, date of birth, citizenship and immigration status, nationality, immigration benefits, immigration history, admission information, customs import-export history, criminal arrest and conviction records, Alien Registration



Number (A-Number), phone numbers, addresses, identification document numbers, criminal associations, family relationships, employment, military service, education and other background information. IDOCX also creates an alpha-numeric tracking number specific to each document that allows both the system and user to identify the investigation or project to which the document pertains.

As described in the Overview, the type of electronic documents that IDOCX can create or import includes but is not limited to: Tagged Image File Formats (TIFF Images), Portable Document Format files (PDF Files), JPEG Images, Microsoft PowerPoint Documents (PPT Files), and Microsoft Word Documents (DOC Files). IDOCX also creates various associated files for every document that is scanned or imported into the system. These files are:

(1) The OCR file: This is a text file created by the OCR Tool which displays the OCR-generated text in the same format as the original document. For instance, if an original document consisted of four paragraphs, the OCR text file will mirror the structure and format of that document, and include four paragraphs.

(2) The Extracted Text file (ET): After the OCR process is complete, the IDOCX system creates an ET file. This text file contains all the text from the OCR text file, but will not have any formatting to allow for more streamlined text searching. The ET file allows IFS and other analysis tools to search the content of the document.

(3) The Machine Translation (MT) file: When a machine translation is performed on a foreign-language document using the Machine Translation Tool, IDOCX creates a separate MT file that is associated with the primary document and includes the English translation. The MT file is created only when an IDOCX system administrator nominates a document for Machine Translation.

(4) The Human Translation (HT) file: In the event a human translator is engaged to translate a document, the HT file will be used to retain the translation. The HT file can also be used to retain a translation of handwritten documents that the OCR tool is unable to process. For every document in IDOCX, even those that are in English and do not require translation, the system creates a Human Translation (HT) file that is associated with the primary document in the system.

(5) The XML file: Following the OCR and Extracted Text processes, IDOCX also creates an XML file that contains a document's metadata. Metadata can best be described as information about the document. For example, if a set of documents relate to a human smuggling case, the IDOCX system administrator may tag these documents as 'human smuggling'. This tag would show in the XML file. If a user in IFS were searching for documents relating to human smuggling, the XML files containing these tags would aid in search capabilities.

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

In most cases, information is obtained from the paper and electronic documents collected during the course of an investigation or law enforcement activity. The sources of the documents vary by case and/or activity but can include documents seized or otherwise obtained from individuals, businesses, government agencies, or organizations. Where IDOCX is supporting non-law enforcement projects, the



sources of the documents are typically internal to ICE or DHS. As mentioned above, these projects typically involve the digitization of existing paper files maintained by the agency.

IDOCX itself is the source of the various associated files (OCR, MT, ET, XML, and HT files) created during document analysis.

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

The primary purpose of IDOCX is to use technology to increase the efficiency and effectiveness of document collection, organization, and analysis. ICE collects, digitizes, and analyzes these documents to assist in the efficient detection, investigation, and prosecution of violations of laws enforced by ICE or other components and offices within DHS. In non-law enforcement contexts, the documents are being collected and digitized to reduce the agency's reliance on paper records and to make agency records accessible and searchable through electronic means.

IDOCX maintains copies of the records for backup purposes. For example, a maintenance issue that may occur is if data sent to IFS was not properly processed by IDOCX. Having the original information remain on the IDOCX system allows system administrators to reprocess the export to IFS to ensure accuracy.

1.4 How is the information collected?

ICE agents typically collect these records during the course of an investigation or other law enforcement activity. The collection of these documents may occur by execution of a search warrant or subpoena, through voluntary production by the source, or other legal means. The ICE agents provide collected documents to the IDOCX team for processing and uploading into IDOCX. In some cases, the IDOCX team will accompany the ICE agent's onsite to scan documents for processing at headquarters.

1.5 How will the information be checked for accuracy?

Inaccuracies may result from errors during the OCR or machine translation processes in IDOCX. To mitigate this risk of inaccurate data, IDOCX associates the original documents with the associated documents (e.g., OCR file) that are created by the system's OCR and language translation tools. These documents are linked and sent to IFS (or returned to the case agent or project manager, if that was the request) in the dataset for the project or investigation. The association of these records – the scanned image of the original document and the OCR or language-translated files – within the dataset helps to ensure accuracy because it allows personnel accessing these records to view and compare the documents to identify any inaccuracies. IDOCX also links digital copies of the original documents to their respective information by tracking numbers assigned during processing.

The accuracy of the information in the actual documents themselves varies depending on the nature of the materials. In most law enforcement contexts, documents that are seized or otherwise collected for evidentiary purposes cannot be corrected and the accuracy or inaccuracy of the documents may be issues of fact for the jury to determine. For example, if ICE seized documents in an investigation



into the production and distribution of fraudulent identification documents, ICE agents would willingly accept inaccurate information contained in the fraudulent documents as that is a critical factual element they must prove to demonstrate the law has been violated. In this example, the fraudulent identification documents processed in IDOCX would not become intermingled with other datasets in IFS. This information would be loaded into IFS as a separate file and access would be restricted to allow only privileged users, usually agents working on that specific case, access to that set of data.

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

ICE has been authorized to collect information under 8 U.S.C. §§ 1103, 1105, 1221, 1225, 1281, 1302, 1303, 1304, 1305, 1306, 1324(b)(3), 1324a, 1324c, 1357, 1360(b); 18 U.S.C. Chapter 27; 19 U.S.C. §§ 1431, 1436, 1481, 1484, 1485, 1509; 1584, 1589a, 1592, 1593a; 21 U.S.C. § 967; 31 U.S.C. §§ 5316, 5318; 40 U.S.C. § 1315; and 50 U.S.C. App. § 2411.

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

Privacy Risk: There is a risk that information generated by the system's tools may be inaccurate and could prejudice the individual to whom it pertains or the individual under investigation.

Mitigation: To mitigate this risk, IDOCX links the system-generated information (OCR results, machine and human translation files) with the original scanned document or electronic record. Users have the opportunity to view the original file and identify any obvious errors. Additionally, any use of the document or a translated version of the document in legal proceedings will require the agency to produce the original record allowing the defendant to independently verify its content or to challenge the translation.

Privacy Risk: There is a risk of retaining more information than is necessary to accomplish the purposes of the law enforcement investigation or activity for which IDOCX is being used.

Mitigation: This risk has been mitigated by the inherent limitations placed on federal agencies that perform investigations and activities in which information is collected and retained for law enforcement purposes. Constitutional and statutory requirements provide safeguards such as the requirement for a search warrant or subpoena before records can be compelled to be produced by private persons. In addition, IDOCX will retain data for the time period specified in question 3.2 of this PIA.



Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The IDOCX documents that are scanned or imported into the system are used for a variety of purposes, including law enforcement investigations, law enforcement activities, and non-law enforcement projects, including agency digitization projects to reduce reliance on paper record systems. The documents may be used by case agents or other personnel to analyze large amounts of data to develop new leads, to organize large numbers of records, and to find specific words, phrases, and records. The OCR files created by IDOCX's OCR Tool are used to produce computer-readable and searchable versions of image files created by scanning physical documents. The MT files created by IDOCX's Machine Translation Tool and the HT files created by the Human Translation Support Tool contain the English translation of foreign language documents which can then be reviewed and used by ICE personnel in the context of the particular investigation, activity or project.

For example, in an investigation into a business owner that is possibly financing human smuggling where a significant volume of the business owner's documents has been collected, IDOCX helps the investigating agents quickly locate important or related records. If the ICE agent working on the case is looking for the specific amount of \$1,600.44, it could take weeks to search seized physical documents to locate that specific amount. By processing the information through IDOCX and loading it into IFS, the ICE agent could simply search the records for '\$1,600.44' and get instantaneous results, allowing the agent to make important connections between financial statements.

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

IDOCX uses several tools to analyze data. First, the IDOCX OCR Tool is used to translate images of documents (i.e., TIFF, PDF, or JPEG files) that contain handwritten, typewritten or printed text into machine-readable data. The OCR Tool is a commercial product that uses well-established optical character recognition technology. By recognizing the fixed shape of different characters in an image file in IDOCX, the OCR Tool "translates" the numbers and letters in the image file into computer-readable and searchable text files. The tool saves the text file and links it to the image file of the document in the IDOCX database server. The OCR text file contains all of the formatting that is in the original document. A separate extracted text file contains the same information without the formatting. These "translations" allow the document contents to be searched electronically for specific words or information. The IDOCX OCR Tool supports 190 languages.

Second, the IDOCX Machine Translation Tool is a government product that automatically translates documents that are in a foreign language. The Machine Translation Tool reads those



documents and provides a translation into English that is stored in a separate file, called an MT file, that is associated with the original document. This tool can perform machine translations of 157 languages.

Third, the IDOCX Human Translation Support Tool supports any human translation of a document from a foreign language into English or translation of a handwritten document that the OCR tool is unable to process. Once a human translator logs into IDOCX, they will have an in-basket that lists their current tasks. If during the standard IDOCX process a user elected a document for human translation, that document will arrive in the human translator's in-basket. The translator will be able to view all the original images of the document, as well as all other documents. Once they are ready to begin transcribing, they will be able to open the blank HT file that was created during the IDOCX processing, and enter their translation.

Finally, IDOCX records that are exported to IFS may be analyzed using the tools in IFS. IFS's analytical capabilities are discussed further in the IFS PIA.³ IDOCX-processed documents may also be returned to the agent or project manager that requested their creation on CD. In those instances, the requestor may have the capability to use stand-alone search tools (such as Windows search, or commercial tools) on a local server to search and retrieve information from the IDOCX records. This storage and search processing occurs locally and is not part of the IDOCX system.

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

IDOCX does not use commercial or publicly available data.

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

Privacy Risk: There is a possible risk of misusing the information in IDOCX.

Mitigation: To mitigate this risk, all users receive a standard IDOCX training course that reviews the basic operating procedures of the system. Included in this briefing is a section covering privacy concerns associated with use of the IDOCX system. In addition, users must undergo the required annual privacy and security training which stresses the importance of authorized use of personal data in government systems.

Privacy Risk: There is a risk that individuals may have access more information than necessary to complete specific tasks.

Mitigation: To mitigate this risk, IDOCX employs role-based access controls so that persons only have access to a limited amount of information and information systems (including specific ports, protocols, and services) necessary for their specific duties in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals. To ensure that authorized users are performing only authorized actions, IDOCX maintains an accurate

³ See www.dhs.gov/privacy and click the link to "Privacy Impact Assessments."



audit trail. IDOCX audit trails are sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected.

To protect against unauthorized access, IDOCX employs strict access controls. IDOCX system administrators control who has access to IDOCX. In order to obtain access, users must make a written request, via email, for access to the IDOCX manager. Once the IDOCX manager approves a user request it is submitted to the system administrators. System administrator verifies the user's identities to determine the necessary/required access rights and roles for the user. All account management (establishing, activating, modifying, reviewing, disabling, and removing accounts) is performed manually by system administrators. There are no automated mechanisms to manage user accounts. IDOCX system administrators have identified account types, established conditions for category membership, and assigned associated authorizations to each account type. IDOCX accounts are reviewed quarterly. IDOCX does not allow guest or temporary accounts. All accounts that have an inactivity period of thirty (30) days are automatically terminated.

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?

Information that is scanned into IDOCX can be broken down into two general categories: Law Enforcement Information, and Non-Law Enforcement Information. Law Enforcement Information refers to the information scanned that supports ongoing law enforcement investigations and activities. Non-Law Enforcement Information refers records related to non-law enforcement projects and programs conducted by ICE or other components and offices within DHS for various purposes. Both of these categories contain two sub-categories:

- **Imported Data:** The electronic documents that are either loaded into the IDOCX system or are created when paper documents are scanned and image files of those documents are created in the system. These are the original data files on which IDOCX system tools will act. These files may include any type of electronic or physical record in multiple file formats as described in Question 1.1 above.
- **Processed Data:** Data that has been created through use of IDOCX system tools. This includes the files generated by the OCR Tool, the Machine Translation Tool, and the Human Translation Support Tool.

During the processing of both Law Enforcement and Non-Law Enforcement Information, System Data is also created. System Data refers to information such as audit logs, which tracks processes carried out by the system and users. Audit logs do not contain any information that has been scanned into IDOCX.



3.2 How long is information retained?

The original information that is collected by ICE is retained pursuant to the retention schedule for the programs that collected the information. ICE proposes that the Law Enforcement Imported and Processed Data be retained in the system for three (3) years, and the Non-Law Enforcement Imported and Processed Data be retained for one (1) year. The retention period is necessary in case there is a need for to reprocess an IDOCX project using system tools.

ICE proposes to retain copies of the System Data for seven (7) years. This retention period is necessary for audit purposes, and to help System Administrators facilitate the reconstruction of events if compromise or malfunction occurs or is suspected.

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 retained in IDOCX.

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: The risk presented is that information may be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: Retention of law enforcement IDOCX data for a maximum of three (3) years is appropriate because of the law enforcement and counterterrorism aspects of the information. Information of this nature is relevant and may be necessary to the DHS mission. To decrease the retention timeframe would significantly decrease the overall effectiveness of the IDOCX system. Retention of non-law enforcement IDOCX data for a maximum of one (1) year is appropriate because of the possibility that the data may need to be re-processed. This retention period is appropriate because it is consistent with the retention periods generally established for criminal investigation records, immigration records, administrative records, and law enforcement intelligence products.



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 routinely share IDOCX data with any other organization within DHS. IDOCX processed information is sent to IFS where it maybe shared with other DHS users who have access to IFS. To limit access to sensitive IDOCX data that is placed into IFS, ICE creates a Community of Interest within IFS which allows only specific authorized IFS users access to the data. This Community of Interest is usually limited to agents working on that specific case. In cases where ICE is working on a joint enforcement initiative with other DHS agencies, such as U.S. Customs and Border Protection, ICE may allow CBP personnel access to the IDOCX data in IFS through the Community of Interest. On an ad hoc basis, IDOCX data may be shared with other DHS components or offices. ICE would first verify that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with that component or office's mission.

4.2 How is the information transmitted or disclosed?

In cases of disclosure using IFS, the Community of Interest process described in Question 4.1 above will be used. In the case of ad hoc disclosures, appropriate safeguards will be used to secure the transmission of information, whether in paper or electronic form, consistent with DHS policies and procedures. Examples of safeguards include hand delivery, encryption, marking, and prohibitions on further disclosure without authorization.

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

Privacy Risk: A risk is presented that information may be shared with DHS components in an insecure manner.

Mitigation: In the event that IDOCX processed information is internally shared, the transmission of data will be through secure DHS network. To further ensure that any possible internal information sharing is conducted within the technical and policy guidelines of DHS and its components, all users are trained annually on security and privacy standards.



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 Office of Intelligence does not share IDOCX data outside of DHS.

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

ICE Office of Intelligence does not share IDOCX data outside of DHS. Information in IDOCX is covered by various SORNs including DHS/ICE-009 External Investigations SORN (Dec. 11, 2008, 73 FR 75452), DHS/ICE-008 Search Arrest and Seizure SORN (Dec. 9, 2008, 73 FR 74732), DHS/ICE-006 ICE Intelligence Records System SORN (Dec. 9, 2008, 73 FR 74735), and DHS/ALL-003 General Training Records SORN (Nov. 25, 2008, 73 FR 71656) depending on the context of the original collection.

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

ICE Office of Intelligence does not share IDOCX data outside of DHS.

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

Since, ICE Office of Intelligence does not share data outside of DHS, there are no risks associated with external sharing of IDOCX data.



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?

Yes, notice is provided via the PIA and, depending on how information was collected and on whom, the following SORNs: DHS/ICE-009 External Investigations SORN (Dec. 11, 2008, 73 FR 75452), DHS/ICE-008 Search Arrest and Seizure SORN (Dec. 9, 2008, 73 FR 74732), DHS/ICE-006 ICE Intelligence Records System SORN (Dec. 9, 2008, 73 FR 74735), and DHS/ALL-003 General Training Records SORN (Nov. 25, 2008, 73 FR 71656) depending on the context of the original collection.

In cases where the collection is in support of a DHS law enforcement purpose, opportunities for the individual to be notified of the collection of information may be limited or nonexistent. In some instances, compulsory legal process such as a search warrant, court order, or subpoena, is used to compel production of the materials to ICE and notice is usually required to be provided to the individual at least concurrently with the collection. Whether notice is provided is highly dependent on the context of the collection of information.

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

In cases where the collection is in support of a DHS law enforcement purpose, opportunities for the individual to decline to provide information may be limited or nonexistent. In some instances, compulsory legal process such as a search warrant, court order, or subpoena, is used to compel production of the materials to ICE. In other instances, individuals may have the opportunity to decline to provide the information. Whether these opportunities exist are highly dependent on the context of the collection of 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 cases where the collection is in support of a DHS law enforcement purpose, opportunities for the individual to consent to the particular uses of information may be limited or nonexistent. In some instances, compulsory legal process such as a search warrant, court order, or subpoena, is used to compel production of the materials to ICE and no opportunity to consent to particular uses is available. Whether these opportunities exist are highly dependent on the context of the collection of 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: A risk exists that individuals may be unaware that their information is collected and processed by IDOCX.

Mitigation: This risk is mitigated by the publication of this PIA and associated SORNs.

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 IDOCX by following the procedures outlined in the applicable SORN that covers the information collected by and processed in IDOCX. Requests for access to information in IDOCX that has been exported to IFS can be made by following the procedures outlined in DHS/ICE-006 ICE Intelligence Records System SORN (Dec. 9, 2008, 73 FR 74735). All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in IDOCX could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

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

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia/index.htm>). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.



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

If individuals obtain access to the information in IDOCX pursuant to the procedures outlined in the ICE Intelligence Records System SORN or other applicable SORNs, 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 ICE Intelligence Records System SORN or other applicable SORNs. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

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

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia/index.htm>). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The procedure for submitting a request to correct information is outlined in the ICE Intelligence Records System SORN or other applicable SORNs and in this PIA in Questions 7.1 and 7.2.

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

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



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

Privacy Risk: A risk is presented that individuals are not aware of their ability to make record access requests for records in IDOCX.

Mitigation: This risk is mitigated by the publication of this PIA, the IIRS SORN, and other applicable SORNs which describe how individuals can make access requests under the FOIA or Privacy Act. Redress is available through requests made under the Privacy Act 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 IDOCX could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

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 the IDOCX system is limited to authorized personnel based on job or project assignment. Primary authorized users are ICE law enforcement agents and analysts. Contract personnel responsible for system development and maintenance have access to the system as well. To gain access to IDOCX, individuals must have a valid need-to-know and related job responsibility, which is verified through their supervisors. Once an access request has been received, the individual must take an initial IDOCX training course, which includes signing the Rules of Behavior governing the system. IDOCX system administrators only grant access privileges to individuals with an ICE network account, which satisfies a check of user's credentials. Once an individual's credentials have been verified, all operations associated with granting access is manually performed by a system administrator. This process is meant to ensure proper attention to access levels. Listed below are the three categories of user access that have been incorporated into IDOCX:

- **System Administrators:** Of the three user categories established for the IDOCX system, system administrators have the highest access level. They are responsible for the daily maintenance of the IDOCX system. System administrators are tasked with all responsibilities associated with user access control. In addition to system maintenance, this user category has access rights to all IDOCX processes such as project creation and search tools.



- **Privileged Users:** This user access category is responsible for the management of IDOCX projects. A Privileged User has the ability to import and modify documents, as well as search and view data within the IDOCX database.
- **General Users:** Of the three user categories established for the IDOCX system, General Users have the lowest access level. This user category may search data within the IDOCX database.

These user categories are based on the concept of least privilege. All user accounts are reviewed quarterly by system administrators to ensure only authorized users maintain access. Access and all user actions within IDOCX are audited and maintained in an audit log.

8.2 Will Department contractors have access to the system?

Yes. Contractors will have access to IDOCX for system development, operations, and maintenance. All contract personnel have undergone extensive background investigations before accessing IDOCX or other DHS systems.

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. All personnel who access IDOCX are required to sign a "Rules of Behavior" agreement, which includes provisions to protect sensitive information from disclosure to unauthorized individuals or groups. After the Rules of Behavior have been signed, authorized users are presented with system-specific training that includes their obligations with respect to the handling and sharing of personal information.

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

The Certification and Accreditation process is expected to be completed in November 2009.

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

IDOCX audit trails are sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. The audit record contains the following information:

- Identity of each user and device accessing or attempting to access IDOCX
- Time and date of the access and the logoff
- Activities that might modify, bypass, or negate IT security safeguards
- Security-relevant actions associated with processing



- All activities performed using an administrator's identity
- Failed log in attempts

The IDOCX Information System Security Officer reviews audit trails regularly. The IDOCX system audit logs will be maintained in accordance with the existing ICE system maintenance policies and procedures. Also, any system security violation or suspected misuse is reported to the Office of the Information System Security Manager (OISSM) in accordance with the DHS security standards, as well as to the ICE Office of Professional Responsibility.

In addition to audit trails, IDOCX encrypts all mobile scanning kits, external hard drives, and local desktop computers used as part of the IDOCX system. The IDOCX application itself employs the use of Access Controls Levels to appropriate limit use access as described in Question 8.1. Due to its nature of operations, IDOCX is currently a standalone system. Because IDOCX has no connections to larger networks or the Internet, this greatly reduces the chances of misuse of data by an outside source.

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 primary privacy risk associated with this system is that personally identifiable information will be used inappropriately.

Mitigation: This is mitigated by system access controls, user training, and audit trail monitoring. All users have had their credentials verified, and are current on Information Assurance training requirements. The system administrators mitigate the risk of PII misuse by manually assigning authorized users to correct user categories. Audit logs are maintained and reviewed to further limit the risk of PII misuse. The system is currently undergoing a security certification and accreditation process that reviews those security mechanisms and procedures that are in place, and ensures they are in accordance with established policy.

Section 9.0 Technology

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

9.1 What type of project is the program or system?

The system is a database application with scanning, data processing, machine translation, and OCR tools supporting law enforcement and law enforcement intelligence objectives pertaining to 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?

IDOCX is currently in the development stage of the ICE Enterprise Architecture Life Cycle Management System. Full deployment is scheduled for October 2009.

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

No.

Responsible Officials

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

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security